科技與工程教育學刊 2020，50(1/2)，49-62
DOI: 10.6232/JTEE.202012_50(1/2).0004

以混沌系統為基礎之物聯網安全資料流

Secure Data Stream of IoT Based on Chaotic System

吳錫聰 副教授
國立宜蘭大學 電子工程學系

Shyi- Tsong Wu
Associate Professor of National Ilan University

摘要

物聯網目前正蓬勃發展，物聯網資料流的安全性是資安的一個新課題。物聯網資料流的安全運算必須具有快速特性與有具良好的效率，而串流加密器具快速運算的優點，常應用於即時通訊的安全，其亦切合物聯網安全資料流的保密需求。混沌理論的輸出序列與初始值相關，其於密碼學之應用具有保密性、效率高、隨機性佳等優點，近來亦常見應用混沌理論於串流加密器的實現。本研究基於物聯網安全資料流的需求，結合不同低維度混沌理論建構金鑰流產生器的基本元件，以強化系統輸出序列的安全性。透過軟體實現產生輸出金鑰流，接著我們以 FIPS PUB 140-1 與美國國家科技標準局 NIST 的 SP 800 對輸出金鑰流作亂度分析，結果顯示，在 FIPS PUB 140-1 的測試方面，過率為 100%；在 NIST SP800 的測試，金鑰流的通過率至少為 92%。此外，我們進一步將此基於混沌系統的金鑰流產生器實現於物聯網系統，我們以物聯網平台 Raspberry Pi 為基礎，以實現一個以混沌系統為基礎的物聯網安全資料流，實作結果顯示在接收端可以解密得到正確的原始明文。

關鍵詞: 物聯網、安全資料流、混沌映射

DOI: 10.6232/JTEE.202012_50(1/2).0004

Abstract

With the rapid development of IoT, the security of IoT is a new topic of information. The secure data stream of IoT requires the characteristics of operation fast, well efficiency, and that is just the advantage of stream cipher. The stream cipher is used for the security in real time communications, and it matches the requirement of the security of secure data stream of IoT. The outputs of chaotic system are highly related with the initial value, high randomness, and high efficiency. It is able to apply to cryptography. Recently the applications of chaotic theorem have been highlighted to enhance the security of stream cipher. In this paper, we combine 1-dementional chaotic systems with other basic elements of stream cipher and construct a hybrid chaotic stream cipher, to promote the period length, randomness, and the linear complexity of the output. After the implementation of stream cipher by Matlab, the output of the cipher will be examined via FIPS PUB 140-1 as well as NIST SP 800 for the randomness. For the test of FIPS PUB 140-1, all the pass rates of the proposed keystream generator are 100%. For the pass rates of NIST SP800-22, the proposed keystream generators is at least 92%. Besides, the proposed the hybrid chaotic based algorithm will be realized in the IoT platform Raspberry Pi for the security in IoT communication and wireless communication practically. From our implementation, the decrypted data is identical to the transmitted data correctly.

Keywords: IoT, secure data stream, chaos system

DOI: 10.6232/JTEE.202012_50(1/2).0004

壹、簡介

隨著科技發展與資訊通訊系統的普及，物聯網(Internet of Things，簡稱 IoT)已成為新的網路科技潮流及趨勢。物聯網創造了一個可以讓很多生活物品藉由網路彼此相連結並整合的世界，而這樣的世界將帶給使用者更為「智慧化」的服務。藉由這些快速而即時的資訊傳遞，提供人們通訊上及資訊需求的即時性與便利性。

串流加密器(Stream Cipher)為目前運用於通訊系統中最常見的加密器，其具有高速加密的特性，並且易於實現。在物聯網資料流的安全保護上，串流加密器自然比對稱式區塊加密器(Block Cipher)優越 0。圖 1 簡單描述串流加密器的加解密步驟，一開始加密程序是由虛擬亂數位元產生器(Pseudorandom bit generator)來產生一個較長的二進制序列之金鑰流(Keystream)，接著將明文與金鑰流做互斥或閘(XOR)運算以產生密文(Ciphertext)，反之則為解密步驟 000。

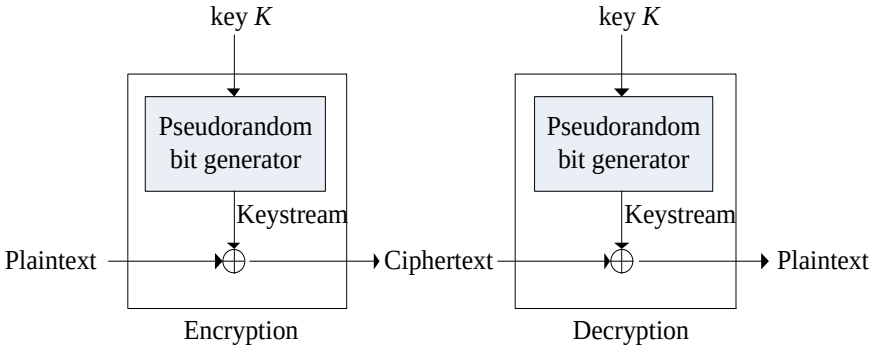

圖 1 串流加密器

近期來講混沌理論(chaotic system)這名詞在這幾年引起眾多學者的注意和研究。著名的學者 E.N. Lorenz 在 1963 年指出混沌系統通常是非線性系統並符合下列幾項特徵，主要有以下特性：非線性、敏感於初始條件、奇異吸引子、系統簡單、回饋和疊代，即為混沌現象 0。英國數學家 Matthews 提出用混沌演算法來對資料加密，在非線性系統科學理論中，混沌理論是一種現代科學結合電腦高速運算的產物，從有限狀態的系統中得到不規律的特性。

混沌理論應用到串流加密的文獻很多，高維度的混沌系統雖較安全，但其具更多的參數，會造成系統過於龐大的運算量 000，低維度的混沌系統其結構簡單，控制參數較少，執行速度快，但安全性較弱易受攻擊。混沌運算的輸出轉為二進制的輸出序列之金鑰流，若每混沌疊代輸出一個位元 0，效率上似乎有待提升。

基於物聯網安全資料流的需求，我們結合低維度混沌理論建構金鑰流產生器的基本元件，採組合方式提高系統輸出序列的週期、線性複雜度與亂度，以強化物聯網資料流的安全。此外，在輸出效率上，我們將每次混沌疊代運算結果產出提高至 64 位元之二進制金鑰流，使

DOI: 10.6232/JTEE.202012_50(1/2).0004

我們所提出的金鑰流產生器更具效率。

本論文第貳段介紹混沌理論的相關知識與原理，接著在第參段，我們提出以一維混沌系統建構的金鑰流產生器，第肆段針對所提之金鑰流產生器作安全分析與亂度測試，我們並說明測試結果，第伍段將所出之提金鑰流產生器在物聯網平台上實現，實際完成串流加密器的加密與解密運作，最後，第陸段是本論文的結論。

貳、相關知識與原理

在國內外研究中，串流加密器和混沌理論的研究不少，以下將針對混沌理論及其在串流加密器的應用，簡略提出說明與探討。

一、 Logistic 映射之混沌演算法

Logistic 映射目前被廣泛應用於混沌加密，其對初始條件有高的靈敏度。定義如下：

$$X_{n+1} = \mu X_n (1 - X_n) \tag{1}$$

式中的 μ 是一個控制參數，X_n 是一個實數且範圍在[1,0]之間，而當 μ 大於 3.56995567 小於 4 時，系統就會進入混沌狀態，Logistic 映射優點是簡單，而且實現容易 0。

二、 Tent 映射之混沌演算法

Tent 映射又稱為帳篷映射 0，是片段線性的一維混沌映射，具有均勻的機率分佈特性。其定義如下所示：

$$X_{n+1} = \begin{cases} uX_n & , X_n < 0.5 \\ u(1 - X_n) & , X_n \geq 0.5 \end{cases} \tag{2}$$

這裡的 u 範圍介於[0,2]之間，而且因為函數簡單，且對系統造成負擔低，因此用於加密時容易實現，因含有混沌系統的特性，因此具備有相當的安全性。

三、 Sine 映射之混沌演算法

Sine 映射函數亦稱正弦映射函數，由於該函數的值域比較特殊，所以可以將自變數以及值域都控制在[−1,1]的區間之內 0。其定義如下式(3)：

$$X_{n+1} = a\sin(\pi X_n) \tag{3}$$

其中的的 a 介於[0,1]之間，該函數的優點在於它的值域可以輕易控制，且疊代次數與平均計算時間也較短，平均誤差也偏低。

四、 高維度混沌演算法

高維度的混沌系統比一維度混沌具複雜的形式和更多的系統參數，相對的它所需要運算量會較大。Hui-yan Jiang 提出一種以三維 Lorenz 混沌系統為基礎的數位影像加密方法 0，使

DOI: 10.6232/JTEE.202012_50(1/2).0004

用系統生成的序列分析和預先處理方法，這使得金鑰流具有良好的統計特性與安全性，高維度的混沌系統雖較安全，但其具更多的參數，恐會造成系統過大的運算量 0。

五、 複合式混沌系統

單一混沌系統其結構較簡單，系統參數也較少，容易被攻擊。而高維度的混沌系統所需要運算量較大，所以為了解決其各自的缺點，並擷取串流密碼和低維度混沌系統之優點，我們使用使用多個低維度混沌系統和不同的參數來構建一個新的系統，一方面可以增加控制參數數量，但卻不會有高維度的混沌系統所造成的系統負擔 00000。

在另一方面，混沌運算的輸出轉為二進制的輸出序列之金鑰流，在輸出效率上，若每混沌疊代輸出一個位元 0，效率上似乎有待提升。在即時通訊系統上，若無法完成快速的加解密運算，則不能達到即時通訊保密的目的，在物聯網的應用上亦是如此。

我們約略介紹混沌理論中比較主流的幾個系統，也從國內外的文獻中，得知大部分都已經成功實現於數位資訊加密，所以如果要研究一種新的串流加密演算法，不能單單光靠單獨種類的系統，而是朝複合系統發展 00，經由組合方式以複合式混沌系統來提升物聯網資料流之安全性。而在輸出效率上，我們設計每次混沌疊代運算產出更多位元之二進制金鑰流，將使其具更佳的效率，在應用上也會有更多的優勢。

參、混沌系統金鑰流產生器

本段將提出一維複合式混沌系統為基礎的金鑰流產生器，首先我們先介紹其架構，接著是由輸入金鑰產生一維混沌系統之所需之初始值與系統參數，最後介紹輸出金鑰流的產生方法。

一、 一維複合式混沌系統

我們實驗之複合式混沌系統，其基本組成元件為一維的混沌映射，我們的電路使用 XOR 元件來結合不同的混沌映射，以下為我們實現的混沌系統基本架構:

- XOR 結合 Logistic 映射及 Tent 映射
- XOR 結合 Logistic 映射及 Sine 映射
- XOR 結合 Tent 映射及 Sine 映射。

(一) XOR 結合 Logistic 映射及 Tent 映射

在本小節，我們介紹 XOR 結合 Logistic 映射及 Tent 映射，如圖 2 所示，圖中 key1、key2 分別是 128 位元的輸入金鑰，l_n 是 Logistic 映射的輸出序列，t_n 是 Tent 映射的輸出序列。二進制序列之 Q_n 是 l_n 及 t_n 經 XOR 運算產生。

DOI: 10.6232/JTEE.202012_50(1/2).0004

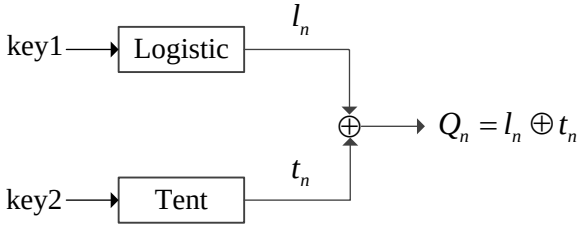

圖 2 XOR 結合 Logistic 映射及 Tent 映射

(二) XOR 結合 Logistic 映射及 Sine 映射

如圖 3 所示 XOR 結合 Logistic 映射及 Sine 映射，在本圖中，l_n 是 Logistic 映射的輸出序列，s_n 是 Sine 映射的輸出序列。二進制序列之 Q_n 是 l_n 及 s_n 經 XOR 運算產生。

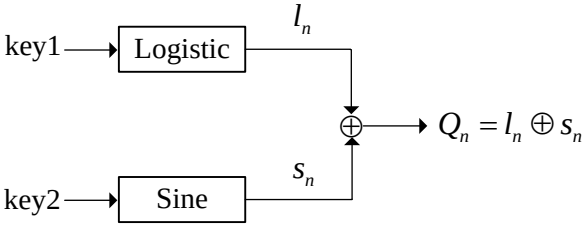

圖 3 XOR 結合 Logistic 映射及 Sine 映射

(三) XOR 結合 Tent 映射及 Sine 映射

Tent 映射及 Sine 映射的結合如圖 4 所示。在圖中，t_n 是 Tent 映射的輸出序列，s_n 是 Sine 映射的輸出序列。二進制序列之 Q_n 是 t_n 及 s_n 經 XOR 運算產生。

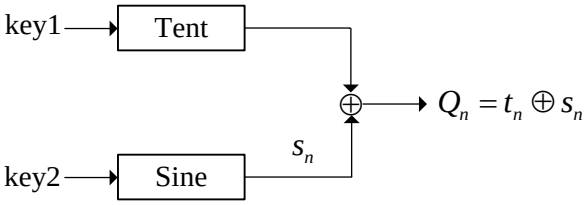

圖 4 XOR 結合 Tent 映射及 Sine 映射

二、 混沌系統之初始值

混沌系統之初始值與系統參數設定由輸入金鑰所決定，首先，混沌系統的輸入為 128-bit 之金鑰，然後將 128-bit 金鑰分成左右兩個 64-bit 之 r_i，作為混沌映射的初始值及系統參數。

由於 Logistic 映射的初始值 X_0 必須在（0,1）之間，所以我們將 r_i 的 64-bit 對應到實數（0, 1）。從 64-bit 資料到實數的轉換方法如下：

$$F_1(r_i) = r_i / 1.8447 * 10^{19} \tag{4}$$

使用相同的方法，設定 Logistic 映射中μ參數，使其對應到 3.569 與 4 之間，其方法如

DOI: 10.6232/JTEE.202012_50(1/2).0004

下：

$$F_2(r_i) = 3.569 + (r_i / 1.8447 * 10^{19}) * (4 - 3.569) \quad (5)$$

同樣的，Sine 映射的初始值 X_0 與參數 a 同方程式(4)與式(5)，Tent 映射的參數μ在 0 和 2 之內，我們透過方程式(6)的 $F_3(\ )$，將 r_i 轉換為其初始值：

$$F_3(r_i) = (r_i / 1.8447 * 10^{19}) * 2 \quad (6)$$

三、 金鑰流輸出

混沌系統的輸出的一個實數，而金鑰流為二進制序列，之間需要實數與二進制的轉換，轉換方法如下:

$$T(X_n) = y_n = X_n * 2^{64} \quad (7)$$

其中，X_n 是混沌系統的實數輸出，y_n 是二進制輸出金鑰流，在此轉換中，將每次的混沌疊代輸出轉為 64 位元的二進制序列。

肆、安全性分析

在本段中，我們將呈現對我們設計之金鑰流產生器所產生的二進制序列所作的亂度統計測試結果。首先，我們忽略輸出序列的前 200 個輸出，原因是避免攻擊者對初始值與系統參數的攻擊，以之提高系統的安全性性。我們採用的測試標準是 FIPS PUB 140-1 與 SP800-22 兩種，以下將對此二測試與結果作進一步的說明。

一、 FIPS PUB 140

FIPS PUB 140-1 基本上有 4 種亂度測試: Monobit test、Poker test、Runs test 與 Long run test 0。針對這些試，我們先任意選 100 個金鑰與 100 個系統參數初值 initial values 來產生 100 個不同的輸出金鑰流，每一個金鑰流有 20,000 個位元，表 1 (a)至(c)分別是是我們所提出的混沌系統的密鑰流產生器輸出的亂度測試結果，從這些表中，顯示針對 FIPS PUB 140-1 的通過率皆為 100%。

表 1　FIPS PUB 140-1 測試結果

(a) 結合 Logistic 映射及 Tent 映射

FIPS PUB 140-1 tests	Pass rate under 20,000 bits/sample
Monobit Test	100%
Poker Test	100%
Runs Test	100%
Long Run Test	100%

(b) 結合 Logistic 映射及 Sine 映射

FIPS PUB 140-1 tests	Pass rate under 20,000 bits/sample
Monobit Test	100%

DOI: 10.6232/JTEE.202012_50(1/2).0004

Poker Test	100%
Runs Test	100%
Long Run Test	100%

(c) 結合 Tent 映射及 Sine 映射

FIPS PUB 140-1 tests	Pass rate under 20,000 bits/sample
Monobit Test	100%
Poker Test	100%
Runs Test	100%
Long Run Test	100%

二、 NIST SP800-22

NIST SP800-22 基本上有 15 種統計測試 0。針對這些測試，我們也是任意選 100 個金鑰與 100 個系統參數初值 initial values 來產生 100 個不同的輸出金鑰流，每一個金鑰流有 20,000 個位元(Bit)。表 2 (a)至(c)則是 NIST SP800-22 對我們所提出的複合式混沌系統之密鑰流產生器輸出的亂度測試結果，從表 2 (a)到(c)中，我們可以發現我們所提出三個不同混沌系統組合之金鑰流產生器的每個亂度測試的通過率至少約為 92%。

表 2　NIST SP800-22 測試結果

(a) 結合 Logistic 映射及 Tent 映射

Statistical tests	*p* value	Pass rate under 10^7 bits/sample
Frequency	0.554774	95 %
Block Frequency	0.562421	96 %
Runs	0.241574	98 %
Longest Runs of Ones	0.632541	99 %
Rank	0.547188	99 %
Discrete Fourier Transform	0.634885	95 %
Non-overlapping Templates Matching	0.514274	97 %
Overlapping Templates Matching	0.542223	97 %
Universal Statistical	0.664214	100 %
Linear Complexity	0.674141	98 %
Seria	0.842154	100 %
Approximate Entropy	0.659858	99 %
Cumulative sums	0.554120	93 %
Random Excursions	0.547114	92 %
Random Excursions variant	0.965841	93 %

(b) 結合 Logistic 映射及 Sine 映射

Statistical tests	*p* value	Pass rate under 10^7 bits/sample
Frequency	0.475125	97 %
Block Frequency	0.354715	97 %
Runs	0.848252	99 %
Longest Runs of Ones	0.752124	97 %
Rank	0.542181	99 %
Discrete Fourier Transform	0.485884	97 %
Non-overlapping Templates Matching	0.745885	98 %
Overlapping Templates Matching	0.475145	97 %
Universal Statistical	0.554854	98 %
Linear Complexity	0.605447	98 %
Seria	0.732014	99 %

DOI: 10.6232/JTEE.202012_50(1/2).0004

Approximate Entropy	0.586220	98 %
Cumulative sums	0.614451	95 %
Random Excursions	0.725150	94 %
Random Excursions variant	0.695478	93 %

(c) 結合 Tent 映射及 Sine 映射

Statistical tests	*p* value	Pass rate under 10^7 bits/sample
Frequency	0.547445	97 %
Block Frequency	0.588545	97 %
Runs	0.614751	98 %
Longest Runs of Ones	0.701421	98 %
Rank	0.410021	98 %
Discrete Fourier Transform	0.554103	96 %
Non-overlapping Templates Matching	0.944745	98 %
Overlapping Templates Matching	0.841221	97 %
Universal Statistical	0.654451	98 %
Linear Complexity	0.741155	98 %
Seria	0.681422	99 %
Approximate Entropy	0.554511	98 %
Cumulative sums	0.515508	96 %
Random Excursions	0.684545	94 %
Random Excursions variant	0.745510	94 %

伍、混沌系統於物聯網之實現

本段中我們將實現物聯網之渾沌密碼的應用。首先我們使用之嵌入式系統是廣為人知的樹莓派，樹莓派同時是一種物聯網平台，它在物聯網中的應用場合是非常多，比如智慧家庭與工業物聯網系統中都有其應用，我們使用其內部提供的 TCP 通訊函式 Socket，完成基於混沌系統之安全物聯網的通訊保密應用。

一、 物聯網發展平台 Raspberry Pi

物聯網的快速崛起帶動相關硬體技術的迅速發展，本實驗我們實做所使用的核心為 Raspberry Pi 3B，它為物聯網之基礎平台之一 0。樹莓派最大的優勢之一在它的軟體方面，其支援的操作系統已經達到幾十種，其函式庫較多，主要開發語言為 Python，並支援各種程式語言，包括 Python、Java、C 等，這為物聯網的軟體開發提供了很大的便利性 0。

如圖 5 所示，為以混沌系統為安全資料流之物聯網系統方塊圖，一開始加密程式是由複合式混沌金鑰流產生器來產生一個長的二進制之序列金鑰流，接著將明文與金鑰流做互斥或閘運算以產生密文，並通過無線網絡進行傳輸數據，反之則為解密步驟。

DOI: 10.6232/JTEE.202012_50(1/2).0004

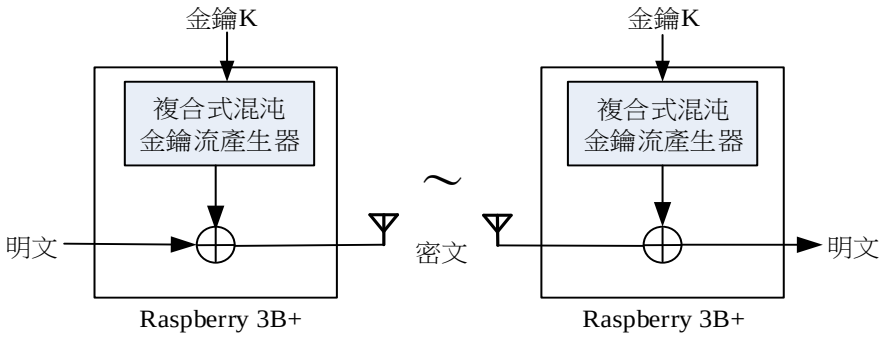

圖 5 以混沌系統為安全資料流之物聯網系統方塊圖

二、 TCP/IP 函式

TCP/IP 為網路傳輸控制協定，socket( )是建立 TCP 通訊的一種函式，它與其他通訊程式的不同是它能實現不同主機間的程式通訊，我們網路上各種各樣的服務大多都是基於 socket 來完成通訊，例如我們每天瀏覽網頁，收發電子郵件等。要解決網路上兩台主機之間的通訊程序問題，首先要標識該程序，在 TCP/IP 網路協議中，主要是依：(1)IP 地址 (2)協議 (3)埠號，來標識通訊程序，用程序標識以建立 TCP/IP 之通訊 0。

TCP 是一種單向連線的傳輸層協議，TCP socket 是基於一種 Client-Server 的程式設計模型。socket 進行通信時，是在伺服器與客戶端之間進行通信，伺服器端監聽客戶端的連線請求，一旦建立連線即可以進行傳輸資料。如圖 6 所示，雙方建立 socket 時都有自己的 IP 位址及埠號，並通過 IP 位址及埠號對應，以保證了送收雙方間的資料傳輸 0。

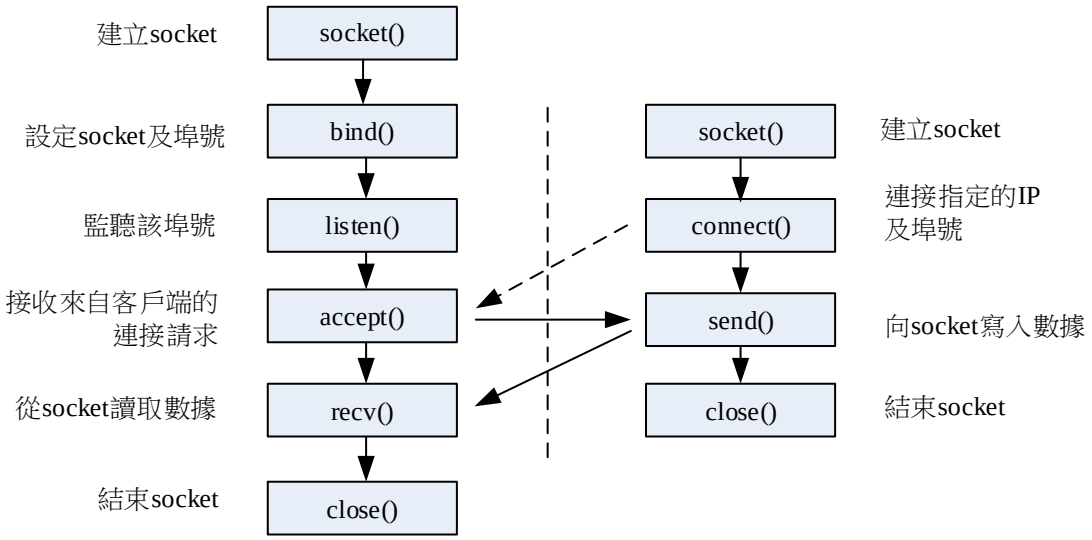

圖 6 送收雙方之 TCP 通訊協定方塊圖

三、 Raspberry Pi 實驗結果

本小節將介紹 Raspberry Pi 的實驗結果。如圖 7 所示為混沌系統初始值及系統參數，左

DOI: 10.6232/JTEE.202012_50(1/2).0004

邊為伺服器端，右邊則是客戶端，本實驗架構以使用 Logistic 映射與 Sine 映射之組合為例。首先介紹 Logistic 映射的部分，key 為我們以隨機產生 128-bit 之金鑰，將 128-bit 金鑰分成左右兩個 64-bit，即 KeyLeft 與 KeyRight，KeyLeft：8d6a8a02547b473f、KeyRight：94b9fe25cd129cf6。KeyLeft 代入方程式(4)得到 Logistic 映射的初始值，KeyRight 代入方程式(5)得到 Logistic 映射的系統參數。在 Sine 映射的部分，金鑰 key 亦為隨機產生之 128-bit，將 128-bit 金鑰分成左右兩個 64-bit ，即 KeyLeft 與 KeyRight，KeyLeft：e065fe2e2b7643b6、KeyRight：82aa1793f4385729。透過方程式(4)即可得到 Sine 映射的初始值及系統參數。伺服器端顯示其 IP 地址:192.168.50.191，接著刪去複合式混沌金鑰流產生器輸出序列的前 200 個，等待客戶端的連接。

伺服器端:

```
Logistic部分
key: 8d6a8a02547b473f94b9fe25cd129cf6
KeyLeft: 8d6a8a02547b473f
KeyRight: 94b9fe25cd129cf6
Logistic映射初始值 : 0.5524069076241008
Logistic映射系統參數 : 3.819395063498118
**********
Sine部分
Key: e065fe2e2b7643b682aa1793f4385729
KeyLeft: e065fe2e2b7643b6
KeyRight: 82aa1793f4385729
Sine映射初始值 : 0.8765562880248234
Sine映射系統參數 : 0.9580963024357582
**********
HOST is 192.168.50.191
1
0x1cb1b631e5f2b000
2
0x43091927d75ea50

 …

199
0x43277db7dd42445f
200
0xbbddd11ef7f58089
Wait for connect
```

客戶端:

```
Logistic部分
key: 8d6a8a02547b473f94b9fe25cd129cf6
KeyLeft: 8d6a8a02547b473f
KeyRight: 94b9fe25cd129cf6
Logistic映射初始值 : 0.5524069076241008
Logistic映射系統參數 : 3.819395063498118
**********
Sine部分
Key: e065fe2e2b7643b682aa1793f4385729
KeyLeft: e065fe2e2b7643b6
KeyRight: 82aa1793f4385729
Sine映射初始值 : 0.8765562880248234
Sine映射系統參數 : 0.9580963024357582
**********
1
0x1cb1b631e5f2b000
2
0x43091927d75ea50

…

199
0x43277db7dd42445f
200
0xbbddd11ef7f58089
```

圖 7 混沌系統之初始值及系統參數設定

雙方經 TCP/IP 連接成功後即可傳輸加密數據，如圖 8 所示。首先雙方儲存 8 個輸出金鑰流，每個金鑰流為 64-bit，且每進行一組傳送、接收後都重新儲存，滿足 8 個未用的金鑰流。由客戶端先進行數據傳送，64-bit 作為一個封包，以“/0”作為結尾符號，之後的填充字元為“0”。每一個封包皆由一組金鑰流進行加密，最後將所有封包一併發送；伺服器端進行接收時，收到的原始數據為密文，會呈現亂碼，計算封包數量後分別進行解碼，解碼完成後將結尾符號“/0”及填充字元“0”捨去，最後顯示出客戶端所傳送之正確數據。

DOI: 10.6232/JTEE.202012_50(1/2).0004

伺服器端:

```
**********
8組金鑰流：
0x25595152b6c4bfaf
0xf8e79b52afcc92fc
0x16f0b369a02c7bc
0x30b96df7729fd023
0x3698a3bc0e448237
0x4f44fb917cd49d4e
0x5b83da9c950c16a5
0xe1f1f5a0ed0f57ff
**********
接收密文： 0x5a53757d5d180106
封包長度： 1
解密後: heLLo/00
做調整後:
[Mon Mar 25 00:58:47 2019] : heLLo
**********
```

客戶端:

```
8組金鑰流：
0x25595152b6c4bfaf
0xf8e79b52afcc92fc
0x16f0b369a02c7bc
0x30b96df7729fd023
0x3698a3bc0e448237
0x4f44fb917cd49d4e
0x5b83da9c950c16a5
0xe1f1f5a0ed0f57ff
> heLLo
明文： heLLo
封包長度： 1
發送密文: 0x5a53757d5d180106
```

圖 8 實驗結果之數據傳輸過程

在物聯網平台樹莓派實現安全資料流的運算效能評估部份，首先我們忽略混沌系的初始化部份，因為此部份可於開機時即完成該運算程序。表 3 分別就我們所提出的混沌架構評估其計算量，而此計算亦正是實現物聯網安全資料流的額外負擔。輸出 64 位元的二進制序需要一次方程式(7)的轉換運算 $T(\,)$，計算量表為 $1T$，兩個混沌序列經一個 XOR 運算得到最後輸出金鑰流，計算量表為 $1XOR$。Logistic 映射一次疊代的計算量為 $2Mul + 1Sub$；Tent 映射一次疊代的計算量，依疊代輸入而定，可分為 $1Mul + 1Sub$ 或 $1Mul$，我們以最差狀況計算為 $1Mul + 1Sub$；Sine 映射一次疊代的運算量為 $2Mul + 1Sin$。由表 3 可發現以平均輸出 64 位元的金鑰流而言，XOR 結合 Logistic 映射及 Tent 映射的混沌架構有較小的計算量，而 XOR 結合 Logistic 映射及 Sine 映射的混沌架構相對有較大之計算量。

表 3
計算量比較

混沌系統	計算量
XOR 結合 Logistic 映射及 Tent 映射	$2T + 1XOR + 3Mul + 2Sub$
XOR 結合 Logistic 映射及 Sine 映射	$2T + 1XOR + 4Mul + 1Sub + 1Sin$
XOR 結合 Tent 映射及 Sine 映射	$2T + 1XOR + 3Mul + 1Sub + 1Sin$

- T：實數對二制 64 位元的轉換運算
- XOR：XOR 運算
- Mul：乘法運算
- Sub：減法運算
- Sin：sine( )函數運算

陸、結論

本文中，我們提出基於混沌系統之通訊加密技術來改良物聯網通訊之安全性，我們的設

DOI: 10.6232/JTEE.202012_50(1/2).0004

計以低維度混沌系統為基礎，並加以整合為複合式混沌系統，我們提出三個組合的之金鑰流產生器，在 FIPS PUB 140-1 的測試方面，實驗結果顯示三個組合的通過率皆為 100%；在 NIST SP800-22 的測試，金鑰流的通過率至少為 92%。

在實作部分，我們也完成了混沌金鑰流產生器在物聯網平台 Raspberry Pi 上的實現，經由所產生之複合式混沌金鑰流與明文作 XOR 運算進行加密，在接收端我們亦使用相同方法解密，實驗結果我們在接收端解密後，可獲得到正確的明文。未來我們的研究方向將朝非線性組合混沌系統方面以創造安全性更佳的金鑰流產生器。

柒、參考資料

賴溪松、韓亮、張真誠（1998）。**近代密碼學及其應用**。松崗電腦圖書資料股份有限公司。

程式前沿。取自 https://codertw.com/程式語言/369901/

玩轉樹莓派。取自 https://kknews.cc/zh-tw/tech/e8ra86q.html

N. W. Abderrahim, F. Z. Benmansour, O. Seddiki (2014, April). A Chaotic Stream Cipher Based on Symbolic Dynamic Description and Synchronization. *Science Business Media Dordrecht*.

M. S. Azzaz, C. Tanougast, S. Sadoudi, A. Dandache (2011). Robust Chaotic Key Stream Generator for Real-Time Images Encryption. *J. Real-Time Image Proc*, DOI 10.1007/ s11554-011-0219-4.

Chen, Li Zhang, Yifang Weng (2010, Dec.). A Data Encryption Algorithm based on Dual Chaotic System. *International Conference on Computer Application and System Modeling*, 431-435.

M. François, T. Grosges, D. Barchiesi, R. Erra (2014, April). A New Image Encryption Scheme Based on a Chaotic Function", *Communications in Nonlinear Science and Numerical Simulation*, *19*(4), 887-895.

HanPing Hu, LingFeng Liu, NaiDa Ding (2013, March). Pseudorandom Sequence Generator Based on the Chen Chaotic System. *Computer Physics Communications, 184*(3), 765–768.

Jaejin Jang, Im Y. Jung, Jong Hyuk Park (2017). An Effective Handing of Secure Data Stream in IoT. *Applied Soft Computing*, *Elsevie*.

Hui-Yan Jiang, Chong Fu (2008). An Image Encryption Scheme Based on Lorenz Chaos System. *Natural Computation of IEEE*, 600-604.

Feng J. Li and X. Yang (2009, Aug.). Discrete Chaotic Based 3D Image Encryption Scheme. *Sympos on Photonics and Optoelectronics*, 1-4.

Jian-Dong, Liu, et al. (2012). Research on Performance of Coupled Tent Map Lattices System. *Fourth International Conference on Multimedia Information Networking and Security*

DOI: 10.6232/JTEE.202012_50(1/2).0004

(*MINES*), 345-348.

E. N. Lorenz (1963). Deterministic Nonperiodic Flow. *J. of Atmos*. Sci., 20, 130-141.

Yongyi Mao, Xiang Chen (2011). An Encryption Algorithm of Chaos Based on Sine Square Mapping. *2011 Fourth International Symposium on Computational Intelligence and Design (ISCID)*, 1,131-134.

Martin Mittelbach, Adolf Finger (2004). Investigation of FCSR-based Pseudorandom Sequence Generators for Stream Ciphers. *Proceedings of the 3rd International Conference on Networking*.

National Institute of Standards and Technology (1994, Jan.). Security Requirements for Cryptographic Modules. *Federal Information Processing Standards Publication* 140-1.

A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray and S. Vo (2008, Aug.). Special Publication 800-22 Revision 1: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *National Institute of Standards and Technology*.

Dixiong Yang, Zhenjun Liu, Jilei Zhou (2014, April). Chaos Optimization Algorithms Based on Chaotic Maps with Different Probability Distribution and Search Speed for Global Optimization. *Communications in Nonlinear Science and Numerical Simulation*, 1229-1246.

J.C. Yen, J.I. Guo (2000). A New Chaotic Key Based Design for Image Encryption and Decryption. *Proceedings of the IEEE International Symposium Circuits and Systems*, 4, 49-52.