工業物聯網加密的串流密碼機制

林政州 [1]、張世豪 [2*]
[1, 2] 淡江大學資訊工程系
[1]606410081@gms.tku.edu.tw、[2] shhchang@mail.tku.edu.tw

摘要

資訊科技(IT)是工業中生產系統和自動化創新最重要的因素之一。在德國，“工業4.0”一詞總結了生產，物流，自動化等工業過程的各種活動和發展。許多研究和開發項目都在不同方面開展工作。從工業與資訊科技產業相關的企業的角度來看，資訊科技產業的資訊安全被認為是目前在智慧製造中很重要的一環。儘管許多當前的資訊科技產業的安全解決方案可以在工業 4.0 中應用，但工業 4.0 中要求的整套系統需要與物聯網結合，增加的是智動化的功能，並結合大數據的分析，提供最佳化的生產流程，並考慮其功能性，即時性，穩定性，節能性，與安全性等諸多因素。其中安全性在目前許多工業 4.0 的設備中仍未整合進去，但卻深深影響整體工廠生產的進度與穩定度，因此極需要在基礎安全機制以及安全架構上完成工業 4.0 的應用。本文在此提出輕量級的工業資料加密傳輸與設備認證的方法，採用的是 WG-8 的加密演算法並改良其尾隨機性，來保護工廠的通訊傳輸。為符合實際工廠的機器設備，我們在實驗中採用 Raspberry Pi3 B+ 做為實驗測試實機，並設計與執行我們所提出的通訊安全加密演算法，實驗結果證明 WG-8 的加密演算法，這會讓 Raspberry Pi3 中央處理器(CPU)使用率提升 40% 運轉，但提供工業物聯網更安全的通訊方式與設備認證。

關鍵詞：工業物聯網、資訊安全、串流密碼法、加密傳輸、設備認證

A Light Weight Stream Cypher Mechanism for IIoT

Cheng-Chou Lin [1], Shih-Hao Chang [2*]
[1, 2] Department of Computer Science and Information Engineering, Tamkang University, New Taipei City 25137, Taiwan (R.O.C.)
[1]606410081@gms.tku.edu.tw, [2] shhchang@mail.tku.edu.tw

Abstract

Information technology (IT) is one of the most important factors in production systems and automation innovation in industry. In Germany, the term "Industry 4.0" summarizes the various activities and developments of industrial processes such as production, logistics and automation.

* 通訊作者 (Corresponding author.)

Many research and development projects work in different aspects. From the point of view of enterprises related to the industrial and information technology industries, information security in the information technology industry is considered to be an important part of smart manufacturing. Although many current IT security solutions can be applied in Industry 4.0, the entire system required in Industry 4.0 needs to be integrated with the Internet of Things, with the added functionality of intelligence and combined with the analysis of big data to provide the most Jiahua's production process considers many factors such as its functionality, immediacy, stability, energy saving, and security. Security is still not integrated in many of the current industry 4.0 equipment, but it has a profound impact on the overall plant production progress and stability, so it is extremely necessary to complete the application of Industry 4.0 on the basic security mechanism and security architecture. This paper proposes a lightweight method of industrial data encryption transmission and device authentication, using the WG-8 encryption algorithm and improving its tailing randomness to protect the plant's communication transmission. In order to comply with the actual plant equipment, we used the Raspberry Pi3 B+ as an experimental test machine in the experiment, and designed and implemented our proposed communication security encryption algorithm. The experimental results prove that the WG-8 encryption algorithm, which will allow Raspberry Pi3 central processing unit (CPU) usage increased by 40%, but it provides industrial Internet of Things more secure communication methods and device certification.

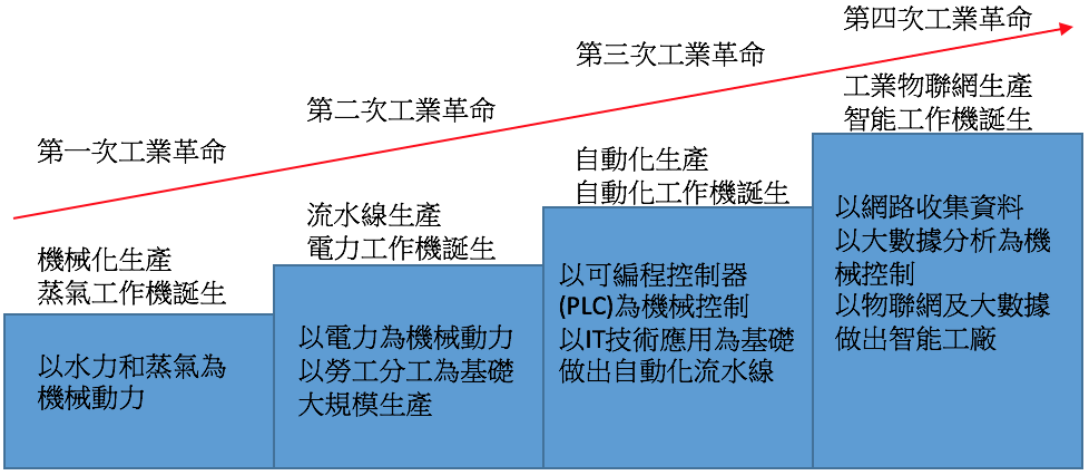
Keywords: Industrial Internet of Things, Information Security, Stream Cypher

壹、前言

1.1 研究背景與動機

工業革命又稱產業革命，一般來說是指在科學技術上有重大突破，使得生產系統加入大量的科學技術改革，讓生產力大幅度的提升，第一次工業革命是 18 世紀由英國發起的技術革命,在科學技術上發明了蒸汽機,在生產系統以蒸汽機為動力製作出工作機,以機械動力取代人力。第二次工業革命在 19 世紀中期，在科技技術上發明電力驅動機械，在生產系統上以電力機器取代原本的機械工作機，更加大了工作機的動力及速度，人類正式進入電器時代。第三次的工業革命，科學技術發明了原子能、電子計算機、空間技術和生物工程，以這三種技術為基礎，大大的縮小了工作機的體積，簡化了工作機的工作流程，大大的減少了工作機的操作流程，我們稱這時代為自動化時代。第四次工業革命，科學技術發明了雲端計算，使得原本在一台電腦不能做的的運算，都可以在網

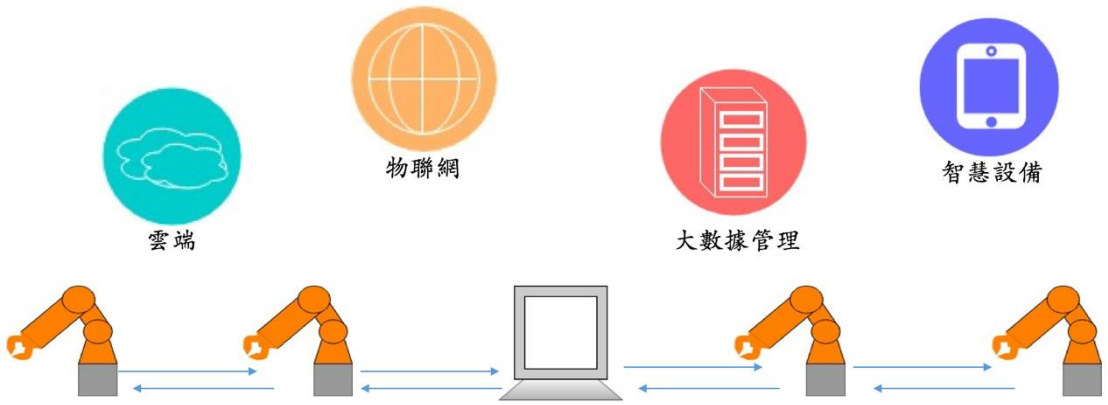
路上運用分散式運算得到解決方案，這促使了物聯網與大數據分析的誕生。[19]



圖一：工業革命演化圖

工業物聯網技術可以在工作機上安裝大量的感測器與聯網設備在工業製造的設備上，並把大量的感測資料傳上雲端平台，並藉由大數據分析找出最適合工廠生產系統的各種數據像是溫度、壓力……等，再藉由工廠的智動化系統修改工廠的溫度、壓力……等資料，提高工廠的生產率與增加效能，這就是智慧工廠，在智慧工廠中可以大量的減少人力資源，以及因為都為感測器做智慧控制，所以也可大量減少工廠意外事故發生。

由上段可知在智慧工廠中，資料傳輸是很重要，因此在智慧工廠中資訊安全比起以往更加的重要，因為一但資料被竊取就會，工廠製作商品的流程就會被發現，更有可能被資料被竄改，導致工廠生產系統停擺，讓工廠損失大量的金錢，例如在 2017 年底位於中東的一間石油工廠突然發生設備故障的緊急事件，導致生產流程被迫中斷，最後調查發現在安全製程系統被植入惡意程式。雖然在目前在使用的資訊安全的演算法可以解決大部分的問題，但還是沒有一種資訊安全的演算法，可以滿足智慧工廠所需的各種要求。另外，在 2003 年，美國核電廠的監控系統遭到 Slammer 蠕蟲感染，導致監控系統將近五小時無法作用。同年，美國的一級鐵路公司 CSX 運輸公司，號誌與調度系統遭到電腦病毒感染，導致旅客及貨物運輸完全中斷。美國也曾和以色列合作研發 Stuxnet 電腦蠕蟲，透過多重零時(Zero-day)攻擊，讓伊朗將近一千部濃縮鈾核子離心機癱瘓，拖延伊朗研發核子武器的發展，可見資訊安全對於工業 4.0 是極為重要的。



圖二：智慧工廠示意圖

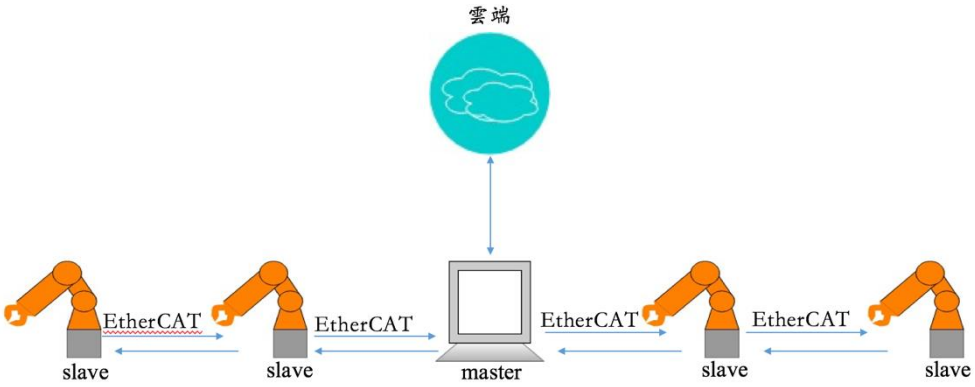
1.2 研究目的

在現在物聯網越來越廣泛使用的趨勢下，工廠中的生產系統也都大幅度的連上網，但在一般電腦使用的資訊安全演算法，並不能滿足工業物聯網的需求，因此在本片論文中主要是針對工廠需求為目的，而設計出加密演算法，以可以確保智慧工廠的資料不會被竊盜、竄改，進而導致工廠機密外流，更嚴重還會導致工廠停擺，因此，本文會透過加密、驗證的方式，來保護工廠的資料。

貳、文獻探討

2.1 工業物聯網

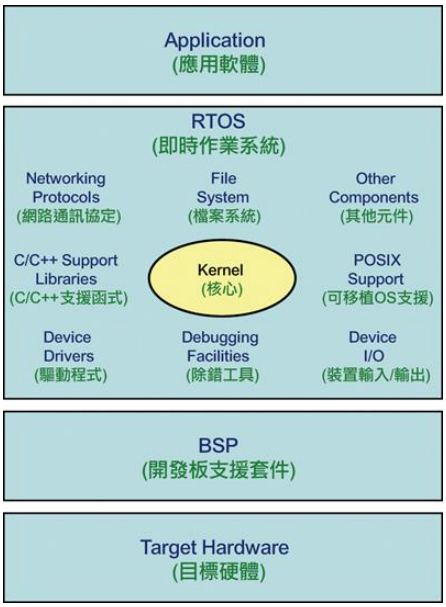
工業 4.0 又稱為工業物聯網(Iindustrial Internet-of-Thing, IIoT)，其中與工業 3.0(自動化工業)最大的差別，就是會藉由工業物聯網的機台上，安裝大量的感測器機台來大量的收集資料，再藉由大數據分析，尋找出最適合生產系統的數據像是溫度、壓力、光照時間……等，因此在工業物聯網的架構中，需要連上網路，將資料傳上雲端，藉由雲端收集大量資料來分析資料，因此工業物聯網比以往的工廠系統更佳的不安全。在工業物聯網的架構中採用主從式架構，由一台主控(Master)電腦來控制多台從屬(Slave)電腦並將資料傳上雲端，主控電腦主要採用 EtherCAT 的傳輸模式來控制機械手臂及感測器，如圖三。



圖三：智慧工廠架構圖

2.2 即時作業系統 (Real-time operating system，RTOS)

在工業物聯網中，即時作業系統為常用到的作業系統，它會按照排序執行、管理系統資源，並為開發應用程式提供一致的基礎。即時作業系統與一般的作業系統相比，最大的特色就是其「即時性」，也就是說，如果有一個任務需要執行，即時作業系統會馬上(在限制的極短時間內)執行該任務，不能有延時的發生。這種特性保證了製造與生產線上任務的即時執行。



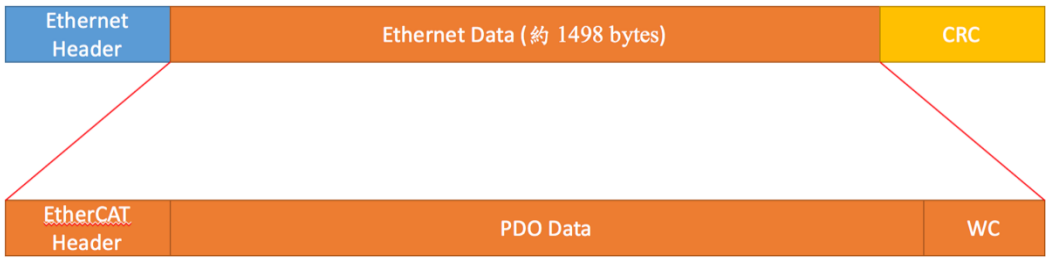
圖四：RTOS 架構圖

在一般功能的處理器市場分類中，若以功能與執行速度來說，大致分為 CPU (中央處理器) > MPU (微處理單元) > MCU (微控制單元)。中央處理器的功能最強，主要應用在電腦產品；微處理單元功能次之，其應用多元，主要應用在嵌入式系統與精簡型電腦

等多種；而微控制單元則是以單一應用為主，應用在各式家電、電子產品、嵌入式產品、穿戴式裝置、物聯網應用產品等控制應用。但由於內部記憶體容量小，因此大型作業系統如 Windows、Linux 等是不可能塞入微控制單元去執行的，且微控制單元大多被應用在即時控制的環境，因此許多容量小的即時作業系統，便成為開發微控制單元軟體的主要平台。[20]

2.3 乙太網控制自動化技術(EtherCAT)

EtherCAT(乙太網控制自動化技術)是一個開放架構，以乙太網為基礎的現場連線系統，其名稱 CAT 是控制自動化技術(Control Automation Technology)字首的縮寫。EtherCAT 最早是由德國的 Beckhoff 公司研發。自動化對通訊一般會要求較短的資料更新時間(或稱為週期時間)、資料同步時的通訊抖動量低，而且硬體的成本要低，EtherCAT 開發的目的就是讓乙太網可以運用在自動化應用中，在工業物聯網中為傳輸方式，EtherCAT 是由 Ethernet 修改而來，實體層一樣都靠乙太網路線，只是在封包的資料中又被切割兩部分，一部分是標頭檔、一部分是資料，標頭檔中含有資料要送達到目的地端的 IP，如圖五，這樣做的目的是為了要加快指令傳輸的時間。



圖五：乙太網控制自動化技術架構圖

2.4 工業物聯網的資訊安全

工業物聯網與傳統工廠再大的差別還有一個特點，就是將設備連上雲端，藉由雲端分析，提高工廠生產量。傳統工廠中只需要防內部人員植入惡意程式，但工業物聯網中並不能只做這種防範，需要設想再將資料連上網後，需要做什麼樣的資訊安全演算法。工業物聯網與傳統物聯網相似，但所需要的資訊安全重點與智慧家居的物聯網又有所不同了，工業物聯網中最害怕的是生產系統癱瘓，因為生產系統癱瘓一天就會導致大量的金錢損失。

工業物聯網系統癱瘓有許多情況，目前最常見為以下兩種，第一種使用分散式阻斷服務攻擊 (Distributed Denial of Service, DDoS)。借助於伺服器技術，將多個電腦並聯起來作為攻擊平台，對一個或多個目標發動拒絕服務攻擊，從而成倍地提高拒絕服務攻擊

的威力，導致系統程式太多無法負荷癱瘓，第二種是主機被入侵，操作指令被竄改，導致在物理現象中發生了系統癱瘓。

2.5 工業物聯網的資訊安全的需求

最常見的解決方法就是，設定容錯率，在機台上設定狀態(例如：溫度、壓力、PH值……等)的門檻值，一但機台收到的指令，是修改裝態低於門檻值或者高於門檻值，可以直接捨棄指令讓機台可以保持，最低限度的生產力，擁有容錯率避免停機。讓生產機台只能在，一定不會傷害產品的情況下工作，工業物聯網中還會發生其他的被網路攻擊情況，像是資料外洩，如果工業物聯網的資料外洩，那其他人就可做出相似的產品，導致工廠商品銷路大量的損失。

在工廠的生產系統中，每一秒就會有大量的產品被生產出來，因此一但生產系統發生錯誤，就需要即時被停機修正，然而在工業物聯網的系統中，遇到錯誤時停機修正是會損失大量金錢的，所以在工業物聯網中會更加要求即時性的修復錯誤，這也是與一般智慧家庭的物聯網資訊安全系統不同的地方。然而在工業 4.0 中，最重要就是要收集大量的資料，所以在機台上會擺放大量的感測器收集資料，但在考慮工廠成本的考量上，機台上的主機大部分都是很便宜的硬體設備，現在又加上收集資料的設備，因此機台所能用的記憶體所剩不多，所以在工業 4.0 的資訊安全系統需要考慮功率為多少。因此論文中的低功耗加密系統，主要就是針對第三種情況的資料保護，會以現有在通訊上常用的串流加密方法改良。以即時性與低功耗的這兩種需求，研究出更符合工業物聯網的架構的資訊安全方法。

2.6 加密演算法

加密演算法是資訊安全中專門用來針對資料保護的演算法，通常會有金鑰及本文和密文，本文使用金鑰經過數學模組就變成密文，並使用密文傳輸，使得別人中途攔截，也只是看不懂的密文，而接收者收到密文，則要通過解密演算法配上金鑰轉回本文，如果加密與解密使用的金鑰一樣，則稱為對稱式加密演算法，如果不一樣，則稱為非對稱式加密演算法，在目前資訊安全的主要使用的加密演算法中，可以區分為兩大部分，區塊加密法及串流加密法：

1. 區塊加密法：使用同一個區塊密碼密鑰對多於一塊的資料進行加密，並保證其安全性。區塊密碼自身只能加密長度等於密碼區塊長度的單塊資料，若要加密變長資料，則資料必須先被劃分為一些單獨的密碼塊。通常而言，最後一塊資料也需要使用合適填充方式將資料擴充功能到符合密碼塊大小的長度一種工作模式描述了加密每一資料塊的過程，並常常使用基於一個通常稱為初始向量的附加輸入值以進行隨機化，以保證安全。

工作模式主要用來進行加密和認證。對加密模式的研究曾經包含資料的完整性保護，即在某些資料被修改後的情況下密碼的誤差傳播特性。後來的研究則將完整性保護作為另一個完全不同的，與加密無關的密碼學目標。部分現代的工作模式用有效的方法將加密和認證結合起來，稱為認證加密模式。雖然工作模式通常應用於對稱加密，它亦可以應用於公鑰加密。

2. 串流加密：串流加密法是以 bit 為單位的加密演算法，加密和解密雙方都使用相同偽隨機加密資料流(pseudo-random stream)作為金鑰，偽隨機意指其數字看視隨機性，但其是因為循環次數太大，一般偽隨機數列一次循環的數列大小要大於10^{40}，所以看不出其循環數值。明文資料每次與金鑰資料流順次對應加密，得到密文資料流。

雖然區塊加密法比串流加密法更加被廣泛使用，但對於智慧工廠其中一項需求時性來說，串流加密法比區塊加密法即時性更高，功耗消耗更低，也因為智慧工廠中所傳輸的資料，都是較短的資料，所以對於區塊加密法一次可以大區塊加密的演算法來說，比較不合適，而針對 bit 為單位加密的串流加密法，比較適合在智慧工廠中使用。

參、方法

串流密碼是最符合智慧工廠的加密演算法，但其中大部分的串流密碼都缺少了驗證性，因此此論文中會去修改串流密碼，利用偽隨機性讓串流密碼可以多一項驗證性，可以得知資料傳輸過程中資料是否被修改。

3.1 串流加密法

在歐盟的 eSTREAM 的計畫中，提出了較符合四種符合智慧工廠的加密演算法都是屬於低功耗的加密演算法，MICKEY、WG-8 [6] 、Grain、Trivium 其中以 WG-8 為保密性最好，WG-8 功率消耗也最低，以即時性來說四種加密演算法都差不多，如表一。[5]

表一：串流加密法比較表

加密法	加密速率 [bits / cycle]	消耗功率 [mW]	throughput [Mbps]	throughput / area	throughput / power
MICKEY	1	8.701	454.5	0.14	52.2
WG-8	1	0.983	500	0.28	508.6

Grain	1	7.772	9876.5	0.56	93.2
Trivium	1	5.186	327.9	0.13	58.4

WG-8 [6] 的加密法，分為兩個步驟，初始化階段及執行階段，在初始化階段中，需要先輸入一組 80bit 的自訂金鑰，假設為K = K_0~K_{79}，及一組隨機產生 80bit 的初始向量 (Initialization vector)，假設為 IV= IV_0~IV_{79}，假設有一組線性位移器 S_0～S_{19}，S_i=($S_{i,7}$~$S_{i,0}$) i=0~19。而 S 是由 K 與 IV 所組成的，$S_{2i} = (K_{8i+3}, \dots, K_{8i}, IV_{8i+3}, \dots, IV_{8i})$，則$S_{2i+1} = (K_{8i+7}, \dots, K_{8i+4}, IV_{8i+7}, \dots, IV_{8i+4})$，則 i=0~9。如以下算式：

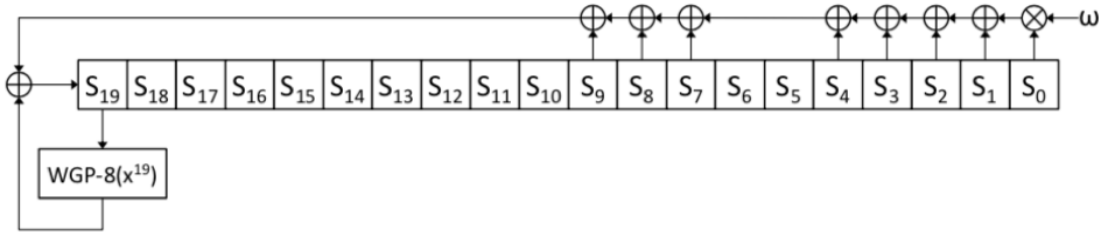
$$S_0 = (K_3, K_2, K_1, K_0, IV_3, IV_2, IV_1, IV_0)$$
$$S_1 = (K_7, K_6, K_5, K_4, IV_7, IV_6, IV_5, IV_4)$$
$$S_2 = (K_{11}, K_{10}, K_9, K_8, IV_{11}, IV_{10}, IV_9, IV_8)$$
$$S_3 = (K_{15}, K_{14}, K_{13}, K_{12}, IV_{15}, IV_{14}, IV_{13}, IV_{12})$$

以此類推…$S_9 = (K_{79}, K_{78}, K_{77}, K_{76}, IV_{79}, IV_{78}, IV_{77}, IV_{76})$

線性位移器會執行 40 次，每次執行到S_{19}時就會進行線性轉換

$S_{k+20} = (\omega \otimes S_k) \oplus S_{k+1} \oplus S_{k+2} \oplus S_{k+4} \oplus S_{k+7} \oplus S_{k+8} \oplus S_{k+9} \oplus Q(S_{K+19}^{19})$，

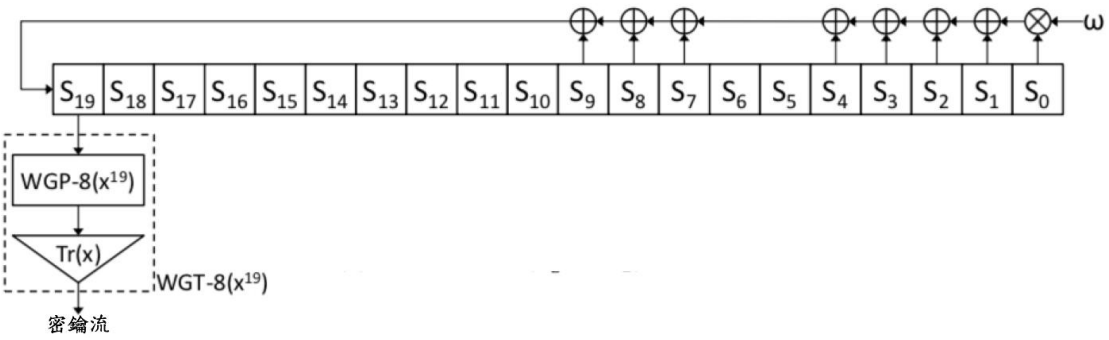
$Q(x) = x + x^{2^3+1} + x^{2^6+2^3+1} + x^{2^6-2^3+1} + x^{2^6+2^3-1}$，$\omega$為陣列基本單位，如圖六。



圖六：初始化線性轉換器

在初始化完後，利用初始化完的 S，就要來製作隨機數的密鑰，在第二步驟中每次執行，每次循環都會產生 1bit 密鑰，而線性轉換器則修改成$S_{k+20} = (\omega \otimes S_k) \oplus S_{k+1} \oplus S_{k+2} \oplus S_{k+4} \oplus S_{k+7} \oplus S_{k+8} \oplus S_{k+9}$，轉換後不會在回到循環當中，如圖七，則 WGT-8(x^d) = Tr(WGP-8(x^d)) = Tr($x^9 + x^{37} + x^{53} + x^{63} + x^{127}$)，Tr(x)=x+x^2+x^{2^2}+⋯+x^{2^7}，$x^d = S_{K+19}^{19}$。

WG-8 的所有運算都是針對金鑰做處理，使金鑰可以擁有偽隨機性。WG-8 的密鑰流的週期為2^{160-1}，在密鑰流的一個週期內 0 的數量只比 1 的數量少 1 是很平衡的，密鑰流的線性範圍為$2^{33.32}$，在後續的步驟中會使用 WG-8 的偽隨機金鑰進行加密與驗證。



圖七：執行時線性轉化器

3.2 加密驗證系統

經由 WG-8 的演算可以得到一組偽隨機金鑰 S，其循環週期為2^{160-1}大於10^{40}，因此可以證明如以 WG-8 的偽隨機數來當作加密金鑰，其加密性是很高的，藉由 S 與本文進行 XOR 生成密文 C，每 11744 bit 做一次加密，因為 EtherCAT 封包資料容量最大可以存 1470bytes 約等於 11760 bit，剩餘 2bytes 為驗證碼，使得封包接收後可以即時性的轉傳。其驗證系統為取S_0~S_7，轉為 10 進位x_0，並在C_{x_0}插入 1 其餘往後遞補，之後再取S_{x_0+1}~S_{x_0+8}，轉為 10 進位x_1，在C_{x_1}插入 1，重複 16 次。

解密前須先檢查，C_{x_0}~$C_{x_{16}}$位置是否為 1，如果為 1，則資料未被修改，如果為 0 則資料已被修改，因該直接都丟棄，如驗證正確，則將 C 與 S 進行 XOR 則變回本文。

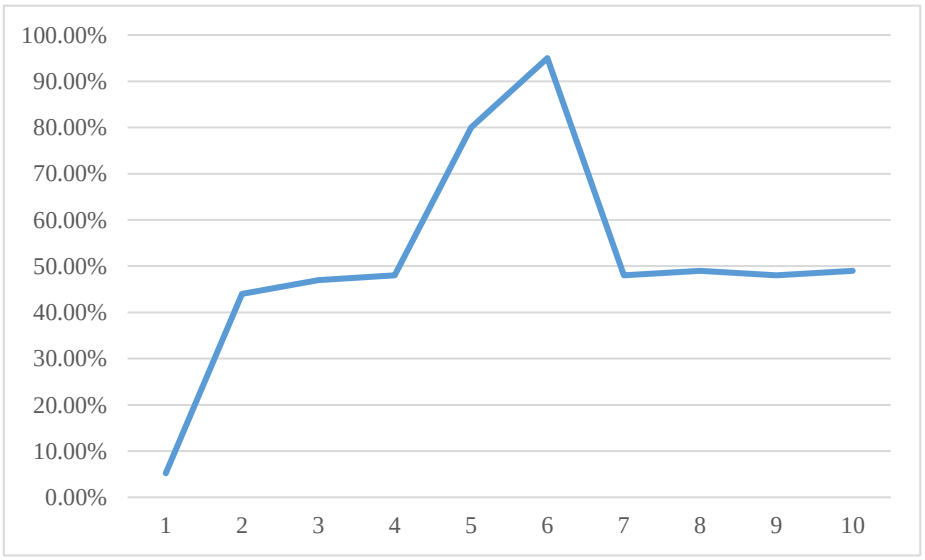
肆、實驗結果

在本論文的實驗中，本論文是採用 Raspberry Pi3 做為實驗測試機器，如圖八，會使用 Raspberry Pi3 為實驗機器的原因是因為，本論文所提出的加密系統，是由雲端加密再由主控台解密，當主控台(Master)需要將資料上傳時，就由主控台機台加密雲端上解密，而主控台機台做為唯一聯網對外的機台，因為其成本的考量，大部分為價格便宜的電腦，因此如果本論文的加密系統在 Raspberry Pi3 可以執行，那在一般的便宜電腦上就都可以執行了，而且其功率消耗不高，因為 Raspberry Pi3 比一般而言比電腦處理效能較差。

4.1 加密驗證系統 CPU 使用率

驗證加密系統的 CPU 使用率為最高為 49%，而當電腦要做資料傳輸時，則衝上了 98%，如圖九，橫軸座標為時間單位是秒。

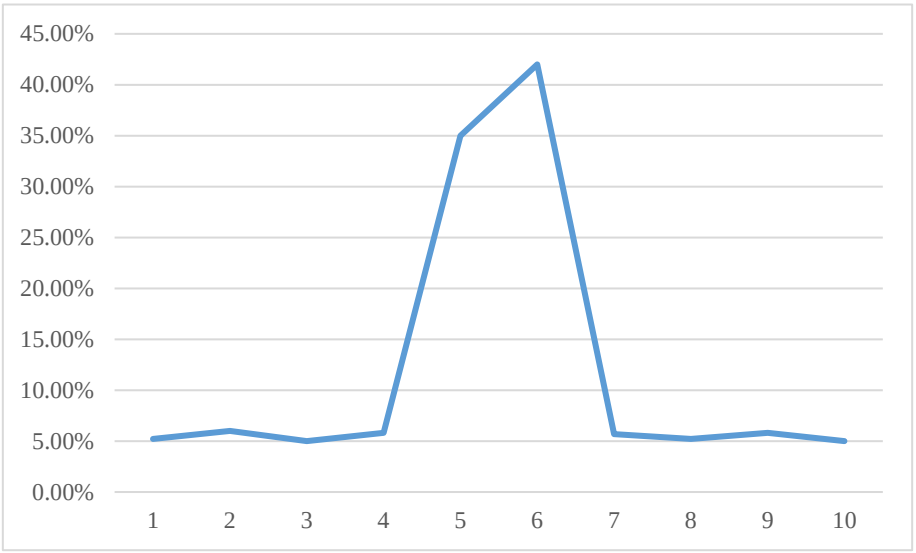
圖八：Raspberry Pi3



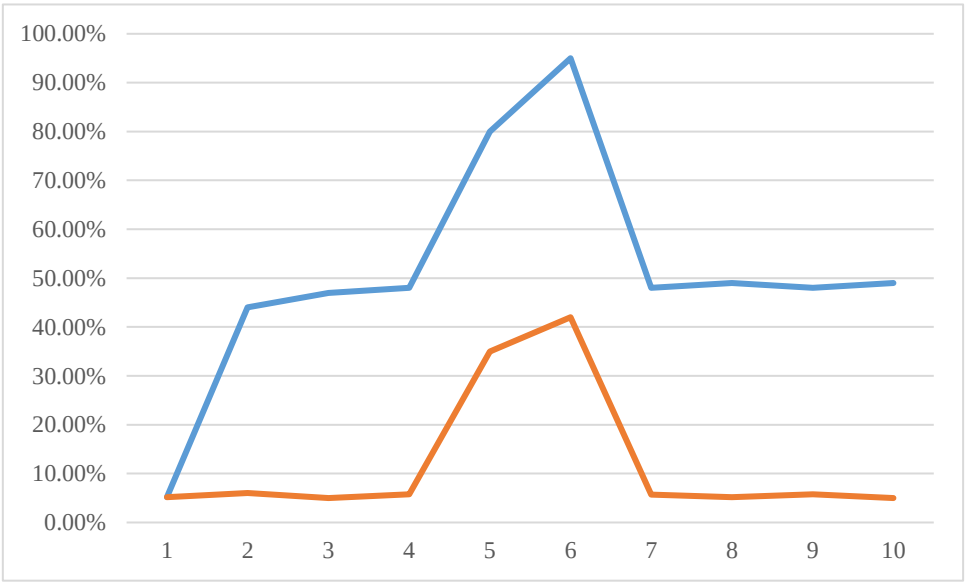
圖九：加密驗證系統 CPU 使用率折線圖

當我們沒使用加密驗證系統時最高為 6%，在做傳輸時最高為 42%，如圖十，橫軸座標為時間單位是秒。

當把兩張折線圖重疊，可以發現雖然資料加密驗證系統，會讓 CPU 使用率提升，但還是可以在 Raspberry Pi3 上執行，中間運算效能差大約是 40%，如圖十一，藍線為有執行加密驗證系統，紅線為無執行加密驗證系統。



圖十 無使用加密驗證系統 CPU 使用率折線圖



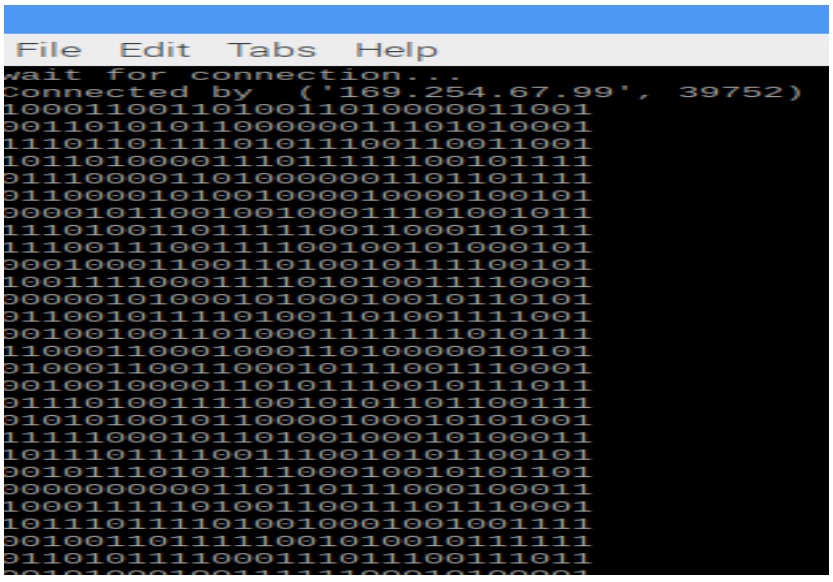
圖十一：整合折線圖

為了要保護資料的加密性，所以在做資料加密驗證系統的機台，一直維持在 47%左右，這 47%就是一直在計算偽隨機金鑰數列，而不是每次要加密資料前才計算，這樣才能確保竊密者取得資料卻不知道其金鑰計算到第幾個偽隨機數，如圖十二。

圖十二：金鑰循環圖

4.2 實驗數據

在這次實驗中，我們用 987654321 數列做為本文，一直重複執行，因此可以得出就算是一模一樣的本文，在偽隨機金鑰的不同，而產生出的密文就不同，如圖十三。



圖十三：密文圖

伍、結論與未來展望

資通訊安全在許多工業 4.0 的設備中目前仍未整合進去，但這卻會深深影響整體工廠生產的進度與穩定度，因此極需要在基礎安全的架構上完成工業 4.0 的建設。本論文使用了 WG-8 加密驗證演算法，WG-8 的所有運算都是針對金鑰做處理，使金鑰可以擁有偽隨機性。WG-8 的密鑰流的週期為2^{160-1}，在密鑰流的一個週期內 0 的數量只比 1 的數量少 1 是很平衡的，密鑰流的線性範圍為$2^{33.32}$，在後續的論文中，我們也使用 WG-8 的偽隨機金鑰進行加密與驗證以符合目前智慧工廠的加密系統的需求，讓智慧工廠擁有加密性、即時性、低功耗、驗證性。未來仍希望能繼續研究相關針對智慧工廠的網路攻擊模式，並加入系統入侵偵測分析與機器學習模式，以提升未來智慧工廠的資通訊安全。

參考文獻

[1] M. Z. A. Bhuiyan, G. Wang and K.-K. R. Choo, "Secured Data Collection for a Cloud-Enabled Structural Health Monitoring System," *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pp. 12-14, IEEE, Dec. 2016.

[2] U. Blocher and M. Dichtl, "Fish: A Fast Software Stream Cipher," *International Workshop on Fast Software Encryption*, pp 41-44, Springer, 1993.

[3] R. Bonnerji, S. Sarkar, K. Rarhi and A. Bhattacharya, "COZMO-A New Lightweight Stream Cipher," *arXiv preprint arXiv:1806.08269*, 2018.

[4] M. Cheminod, L. Durante and A. Valenzano, "Review of Security Issues in Industrial Networks," IEEE Transactions on Industrial Informatics, vol. 9, Issue 1, Feb. 2013.

[5] L. Diedrich, P. Jattke, L. Murati, M. Senker and A. Wiesmaier, "Comparison of Lightweight Stream Ciphers: MICKEY 2.0, WG-8, Grain and Trivium".

[6] X. Fan, K. Mandal and G. Gong, "WG-8: A Lightweight Stream Cipher for Resource-Constrained Smart Devices," *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, pp 617-632, Springer, 2013.

[7] G. Gong, and A. M. Youssef, "Cryptographic Properties of the Welch–Gong Transformation Sequence Generators", *IEEE Transactions on Information Theory*, pp. 2837-2846, IEEE, Nov. 2002.

[8] M. Hamann, M. Krause and W. Meier, "LIZARD – A Lightweight Stream Cipher for Power-constrained Devices," *IACR Transactions on Symmetric Cryptology*, pp. 45–79,

2017.

[9] Z. Li and G. Gong, "On the Node Clone Detection in Wireless Sensor Networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 21, issue 6, pp. 1799-1811, Dec. 2013.

[10] K. A. McKay, L. Bassham, M. S. Turan and N. Mouha, *Report on Lightweight Cryptography*, National Institute of Standards and Technology, 2017.

[11] S. Misra, M. Maheswaran and S. Hashmi, *Security Challenges and Approaches in Internet of Things*, Springer, 2017.

[12] M. Naor, "Bit Commitment Using Pseudo-Randomness," *Conference on the Theory and Application of Cryptology*, pp. 128-136, 1989.

[13] S. Raj and R. R, "Descriptive Analysis of Hash Table Based Intrusion Detection Systems," *2016 International Conference on Data Mining and Advanced Computing (SAPIENCE)*, pp. 16-18, IEEE, Mar. 2016.

[14] A.R. Sadeghi, C. Wachsmann and M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things," *Proceedings of the 52nd Annual Design Automation Conference*, ACM, 2015.

[15] M. Usman, I. Ahmed, M. I. Aslam, S. Khan and U. A. Shah, "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, No. 1, 2017.

[16] N. Wattanapongsakorn, P. Sangkatsanee, S. Srakaew and C. Charnsripinyo, "Classifying Network Attack Types with Machine Learning Approach", *7th International Conference on Networked Computing*, pp. 26-28, IEEE, Sept. 2011.

[17] W. Wu, S. Wu, L. Zhang, J. Zou and L. Dong, "LHash: A Lightweight Hash Function," *International Conference on Information Security and Cryptology*, pp 291-308, Springer, Oct. 2014.

[18] C. Yin, Y. Zhu, J. Fei and X. He, "A Deep Learning Approach for Intrusion Detection using Recurrent Neural Networks," *IEEE Access*, pp. 21954-21961, IEEE, 2017.

[19] http://www.twgreatdaily.com/cat77/node1562986 (2017/10/15).

[20] https://www.digitimes.com.tw/iot/article.asp?cat=130&cat1=45&cat2=25&id=0000424643_ee45qu335sxgr42fqo53o (2018/6/18).