國防部 113 年度「補助軍事院校教師（官）從事學術研究」

四軸無人機加密系統之軍事應用開發與驗證

結案報告

執　行　單　位：空軍航空技術學院飛機工程系
研究計畫主持人：助理教授 劉建均 中校

中華民國　113　年　12　月　05　日

研究計畫書目錄

圖目錄

提要

近年來隨著無人機協助軍事作戰應用的蓬勃發展，使得無人機的技術更加受到了重視，並且軍事作戰當中的資訊安全亦是國防科技領域中相當重要的一環。因此本計畫提出利用無線傳輸的方式來傳輸無人機啟動控制的實際應用，並且在控制訊號的傳輸過程中，為了避免遭受惡意人士的進行資料竊取，我們使用了 RSA 加密演算法技術，來防止無人機的控制訊號在傳輸過程中遭受到資訊攻擊，來加強無人機載具在控制時的資訊安全問題，進而強化無人機資訊傳輸的安全防護。我們利用無線傳輸的即時性及方便性，整合 RSA 加密演算法來進行資料加密與解密，並進行機電整合設計，以改善無人機控制飛行的資訊安全性。

第一章 計畫內容：

第一節 研究緣起與背景：

資訊安全是國防科技相當重要的一環，隨著無人飛機、電子電機科技領域的快速發展，使得無人飛機受到國防武器廣泛的應用，例如戰場攻擊、空中拍攝、空中運送、情資蒐集等運用，尤其以戰場攻擊及空中情蒐偵察為作戰首要任務之一。近年來在軍事作戰當中，為有效降低人員受損的情況下，利用無人飛機來進行各種軍事作戰任務，並配合戰術應用的不同層面，使得無人飛機在作戰應用層面上顯得更加多元化。

然而無人飛機在系統架構上採用的典型方法主要可分為兩個部分，第一個是遠端控制的無人飛機裝置，第二個是地面控制站台。因此，地面控制站台透過無線傳輸方式來進行遠端的無人飛機控制，則需要透過無線傳輸的方式來進行控制訊號的資料傳遞。假設無人飛機與地面控制站進行遠端數據資料的傳輸過程中，若無線訊號數據遭受惡意人士或是敵軍技術人員的竊取或篡改，可能將影響軍事作戰情傳的安全性和機密性。因此對於國防軍事科技上來說，資訊安全是必須考量的重要議題。其中，市面上所販售的無人飛機幾乎都是不具備加密性的飛行控制裝置，欠缺資訊安全保護措施，所以地面控制站所下達的指令在無線傳輸的過程當中，是不具備資訊保護並且容易遭受到惡意人士的竊取，例如：地面站需要對每架無人機裝置的狀態進行監測，如電壓、溫度、傳感器狀態、定位資訊等等，尤其是無人飛機的位置訊息，是相當重要的資訊之一，如何保護無人飛機的控制訊號與狀態資訊，將會是一個重要的問題。

因此我們提出利用無線傳輸的方式來下達控制無人機指令的方法，並且在開放式的飛行控制板上，利用 RSA 資訊加密方法來強化無人機飛行控制之資訊安全問題，並透過訊息佇列遙測傳輸(MQTT)的傳輸方式，來進行我們所下達的動作指令，使動作指令在無線網路的傳輸過程當中是具有加密性質，在控制無人機的過程當中，可以降低敵人或是惡意人士對於資料指令竊取的風險。在設計硬體實作方面上，使用無人機來進行飛行控制訊號的接收及解密功能，而地面控制端可以設計 RSA 資訊加密方法來進行資料加密(密文)，同時透過無線網路下達啟動指令，過程當中皆是傳輸密文指令來進行保護，來達到啟動無人機的效果，目的在於使無人機的控制指令具有資訊保密安全的功能，並達到智慧安全的防護手段。

計劃執行時間預計為一年，執行內容包含無人機之控制系統製作、無線傳輸系統建構、RSA 加密演算法建立以及整體機電系統整合作業，本計畫所得成果，在學術上，可更深入軍事無人機的發展應用，並可建構於教學實踐上，使學生具有資訊安全觀念及無人機基本知識，建立無人機工程應用發展，實作驗證密碼學教學經驗、機電控制整合應用及資訊安全的設計方法參考。

第二節 研究目的及研究重點

2.1 研究目的：

系統研究設計目的就在於運用 RSA 加解密演算法的方式，來將操作者所設定的控制資料進行解密運算，讓有心人士無法輕易干擾或造成竊取事件，控制指令在經過 RSA 加、解密方法後，控制指令仍可以與操作者所設定之指令完全相同，也就是說解密者需具私鑰才能將控制指令成功解密還原，因此惡意人士無法輕易地破解出我們所設定的私鑰密碼，達到以軟體編碼方式的保護功能。

2.2 研究重點：

(1)資訊安全基本特性：

在資訊的安全性威脅問題當中，主要可分成攔截、中斷、欺騙等分類，這些威脅是從資訊網絡中竊取私人信息，或是進行中斷目標從服務裝置中獲得的資訊，以及欺騙目標接受虛假數據，使在未經過目標授權的身份中，進行資料訪問和篡改系統資訊，為了防範這些威脅系統安全性的方法，可以使用訪問權和密碼學的控制方法。權限詢問的安全方法指的是在系統中誰的身份具有可以詢問內部資訊的問題，來防止未經授權的身分進行資訊修改或資源揭露的行為，使用身份驗證和授權機制來防止未授權的外部觀察者竊取資訊，解決此類的安全遭威脅的問題[1][2]。另外一種常被使用的方法為密碼學(cryptography)加密手段，此方法是用於信息安全方法中最古老和最常使用的技術之一，在密碼學的加密演算法當中，可以分為對稱式密鑰密碼方法和非對稱式密鑰密碼方法。加密演算法的基本操作過程就是將原始狀態的數據(即明文)，經過加密演算法進行資訊加密之後，將原始資料數據進行成外部觀察者無法理解的資訊方式，來解決資訊隱私與安全性問題[3][4]。非對稱式加密方法就是每個使用者都擁有一對金鑰：公開金鑰(Public key)及私密金鑰(Private key)，公開金鑰能被廣泛的發佈與傳遞，而私密金鑰則必須被妥善的保存。所以訊息可以使用公鑰進行資料加密，而使用私鑰來進行資料解密，也可以是使用私鑰加密，而使用公鑰進行解密，但不管是使用哪種方式其中鑰匙必須是完整一對的。每個系統設備的資料傳輸安全性在系統當中都是相當重要的，因此我們可以透過加密演算法來對系統控制的信息進行加密，藉以保護原始的控制資料數據。其中最常見的非對稱式加密方法是 RSA 加密演算法、ElGamal 加密演算法以及 Paillier 加密演算法[3][4][5]。

本計畫使用的是 RSA 加密演算法，是屬於一種非對稱加密算法，其優點是無法簡單計算破解使用者所設計的私鑰方法，由於沒有即時有效的方法可以快速分解計算出非常大的次冪整數(或是暴力運算破解)，因此 RSA 加密算法具有良好的加密安全性與可靠性，而 RSA 加密系統主要是使用解決因式分解問題。因此我們利用密碼學的方法來進行設計與驗證，並且達到無

人機的遠距無線網路的控制訊號資料傳輸，同時使控制訊號具有加密性質，確保使用者的資訊不被竊取。

(2)RSA 加密演算法之原理與應用

RSA 加密演算法是一種非對稱加密演算法，在公開金鑰加密和電子商業中被均被廣泛使用。而 RSA 的名稱則是由羅納德·李維斯特（Ron Rivest）、阿迪·薩莫爾（Adi Shamir）和倫納德·阿德曼（Leonard Adleman）一起提出的，其中 RSA 則是由他們三人姓氏開頭字母拼湊而所組成的。公開金鑰密碼學（Public-key cryptography）也稱非對稱式密碼（Asymmetric cryptography）是密碼學的一種演算法，它需要兩個金鑰，一個是公開密鑰，另一個是私有密鑰，其中就是使用公鑰來作加密運算，而私鑰則用作解密運算，如圖 1 所示。因此簡單來說，使用公鑰把明文加密後所得的密文，只能用相對應的私鑰才能解密，然後得到原本的明文，最初使用來做加密運算的公開鑰匙是不能作為解密運算使用，由於加密和解密需要兩個不同的密鑰，故被稱為非對稱加密。當中的公開金鑰是可以公開，並任意向外發布，但是私有金鑰是不可以公開發布，必須由用戶端自行嚴格秘密保管，絕不透過任何途徑向任何人提供，同時也不會透露給通訊的另一方所知悉。

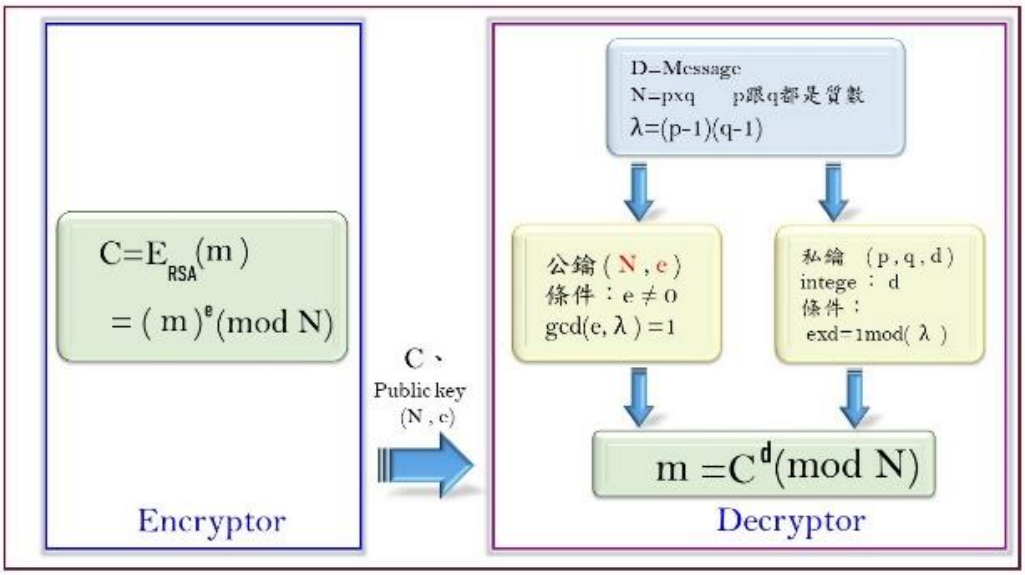

圖1：RSA 加密演算法架構

(3)無線資料傳輸工作原理：

本計畫使用的方式是為 MQTT 網際網路傳輸協定(Message Queuing Telemetry Transport)，MQTT 是一種網際網路佇列訊息傳遞的協議。它的設計上是基於發佈及訂閱的訊息協定模式，其中以輕巧、開放及簡易為設計主軸方向，當系統運作程式容量空間有限或是

網路頻寬遭受到限制的時候，將更具突顯出 MQTT 的優勢。因此，例如連續性的感測資料像是溫度、濕度、壓力、水位、電力監控資料等，都是適合應用 MQTT 監控的資料，因此次被多次使用到工業管理設計層面，所以可以作為控制訊息持續更改的情況下，傳遞到網際網路上。在 MQTT 的通訊協議中，主要有三種角色:發佈者(publisher)、訂閱者 (subscriber)、以及伺服器(Server)，其中發布者必須先行建立一主題訊息，而訂閱者必須針對具相對應需求的主題進行訂閱，而當發佈者在主題區內發布資料訊息後，伺服器就會轉發訊息給所有訂閱該主題頻道的訂閱者，因此可以透過 MQTT 來規劃具有簡易式網際網路資訊安全的功能，以進行雲端網路的資料傳輸。

第三節 研究架構

本專案計畫之研究主題包括：(1)無人機系統架構設計；(2) 無線網路傳輸架構設計；(3) RSA 加密演算法設計；(4) 系統機電整合開發。各研究主題之執行，由本校一般學科部飛機工程系負責各項設計、分析及實驗工作。編組架構如圖 2 所示。

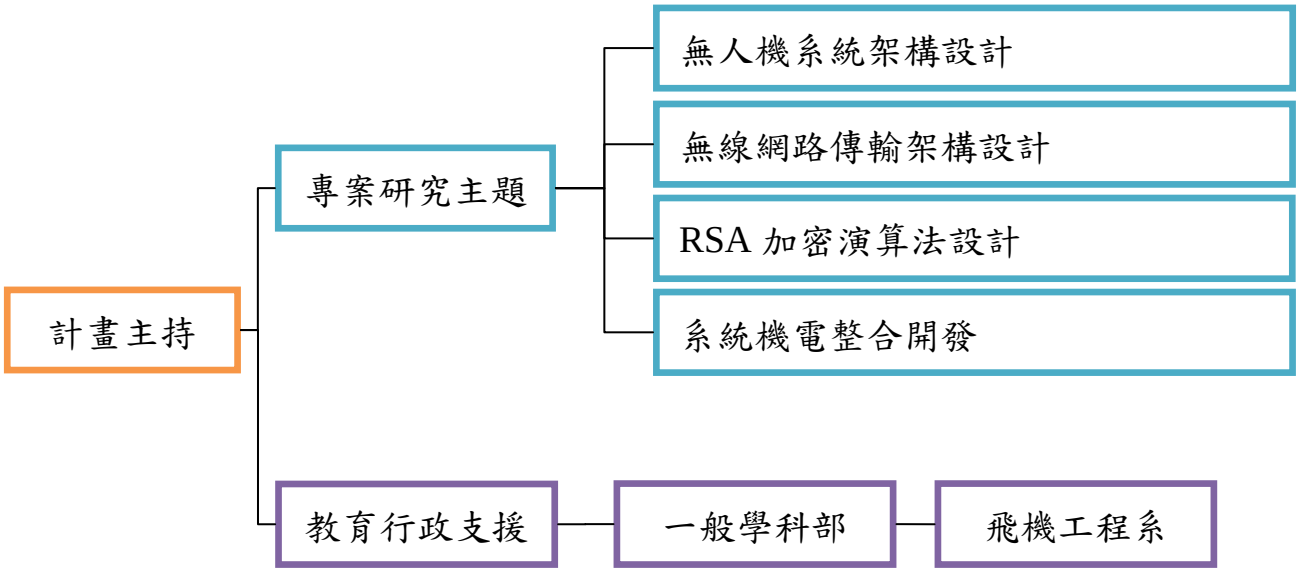

圖2：計畫編組架構

實驗架構如圖 3 所示，使用者透過操控主控端電腦，來設定無人機所要的控制指令，設定好控制訊號後，透過網際網路傳輸協定(MQTT)來將設定好的控制訊號傳送到網路上，由於主控端電腦使用者所發送的控制資料，是以 MQTT 傳輸協定方式傳送到無線網路上，所以可以透過傳輸加密後的控制訊號，來遠端控制無人機裝置。

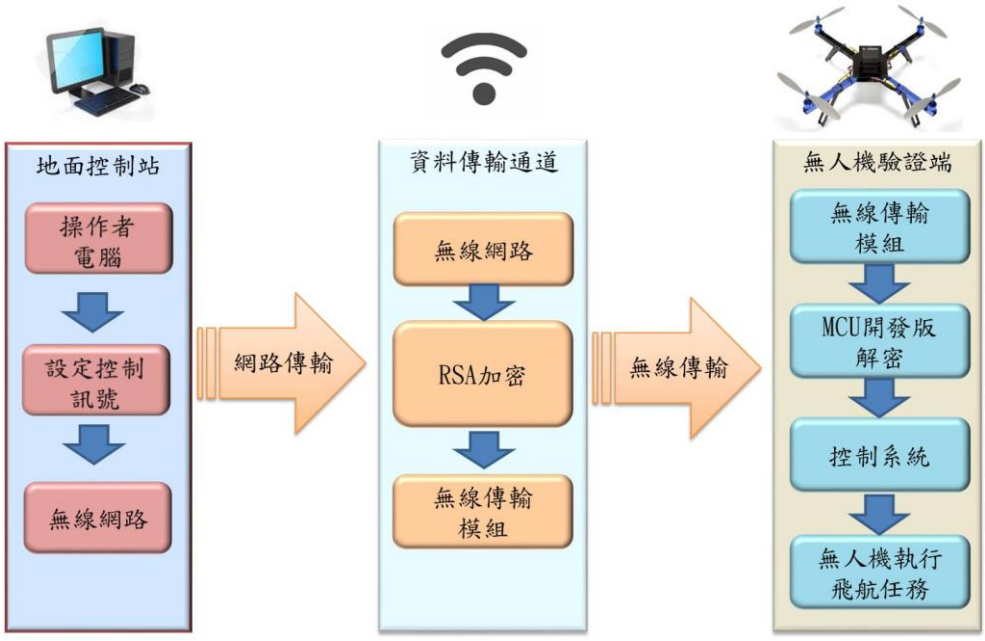

圖3：實驗架構圖

第四節 研究方法及步驟

本計劃之時程預計為一年。第一階段為建立 RSA 加密演算法及 MCU 開發版程式架構設計，來驗證加密演算法及解密資料的正確性；第二階段執行無線網路傳輸架構及系統整合設計，為了使資料能順利傳遞到無人機端，執行資料傳輸時必須確保雙向傳輸設定需一致，並進行資料驗證的可視化展現，了解當無人機接收到加密資訊時，資料的狀態是否符合資訊的保密性，進而達到遠端控制無人機端的效果；第三階段則逕行成果報告製作。研究進行步驟如圖 4。

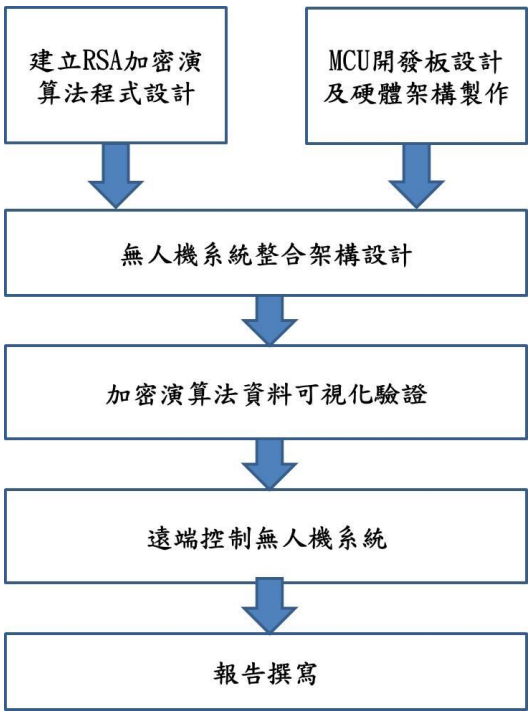

圖4：計劃執行方法與步驟

本研究預劃於空軍航空技術學院進行相關實驗，所使用各項實驗硬體設備目說明如下：

◆ 四軸機實驗設備

四軸無人機是一種輕巧、靈活、易於操控的飛行器。它通過四個獨立的螺旋槳來實現飛行，並且具有高度的機動性和穩定性，如圖 5 所示。為了控制這些飛行器，需要使用一個遙控器，也稱為發射器。遙控器是一種具有無線通信功能的設備，可以將命令傳達到四軸無人機上。在這種情況下，通常使用的無線通信技術是 2.4GHz 或 5.8GHz，這兩種頻率可以提供足夠的帶寬和範圍以進行遠程控制。遙控器的設計通常包括兩個關鍵元素：發射器和接收器。發射器是一個手持設備，通常由一個或多個操縱杆、按鈕和開關組成。操縱杆可以向上、向下、向左或向右移動，從而控制四軸無人機的飛行方向。按鈕和開關可以控制飛行器的其他功能，如啟動/停止、拍照/錄像等。

圖5：四軸無人機

◆ MCU 晶片模組

MCU (MicroController Unit)我們稱為單晶片，在嵌入式系統中，MCU 為組成電路的核心零件，如圖 6 所示。MCU 單晶片是一種智慧半導體積體電路，由處理器、記憶體模組、通信介面和周邊裝置所組成，其中應用範圍非常廣泛，從機器人、無人機、無線電或是車用電子。MCU 具有處理器元件，但它不僅對二進位的數值進行運算，其中還可透過其內建的通信介面和周邊裝置來進行資料傳輸；就技術上來說，MCU 是透過執行儲存在非揮發性的記憶體模組中的程式指令來進行運算，並且由於快閃記憶的技術，促使 MCU 在使用上更加的方便，可隨時進行程序指令的儲存與變更。MCU 是依據使用者的程式編寫邏輯，來進行實體上的功能驅動輸出，達到使用者所設計的需求結果。

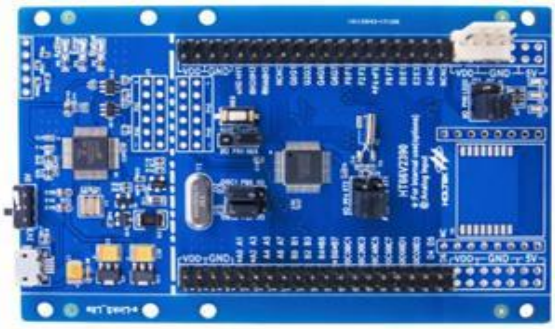

圖6：MCU 微控制器

◆ 飛行控制系統

飛行控制系統一般簡稱為「飛控板」，其中內部會裝設控制器、陀螺儀、加速度計和氣壓計等傳感器。無人機便是依靠這些傳感器來穩定機體，再配合 GPS 及氣壓計數據，便可進行無人機的路徑規劃。我們所使用的四軸無人機飛行控制板是 Pixhawk，它是一款由 PX4 開源項目設計並由 3DR 公司製造生產的自動駕駛儀系統，如圖7所示；其前身是 APM，由於 APM 的處理器已經接近滿負荷，沒有辦法滿足更復雜的運算處理，所以採用了 32 位 ARM 處理器，以 ST Microelectronic 的處理器及傳感器技術進行即時操作的系統，使四軸無人機具有出色的動作性能、靈活性和可靠度。

圖8：開源飛行控制板

◆ 可能遭遇之困難及解決途徑：

我們利用具 MCU 晶片來連接無線傳輸訊號，並接收來自 MQTT 傳輸協定上的控制訊號資料，以 UART 傳輸介面將資料傳遞至單晶片後，將控制資訊(明文)以 RSA 加密進行加密運算，因此若 RSA 加密演算法發生計算錯誤或是資料傳輸錯誤，即無法進行正常的解密運算(造成資料暫存器溢位)。

進行步驟與執行進度如下：

第一階段

1.設計無人機系統架構，以四軸無人機為機體架構進行機架組裝，藉此建立無人機實驗機體設備與驗證。

2.測試無人機馬達與飛行控制板的設定，以電調(電子變速器)來達到機翼動作的控制，進行機體機電控制的基本整合，以利後續應用與測試。

3.遙控器建置藉以接收到使用者所操作動作的遙控指令訊號；因此四軸無人機最少需要具有 4 個不同頻道來傳送無人機的動作指令訊號，以便控制電調控制器，進而控制馬達的轉速。另外可以裝設數據無線傳輸模組，來進行無人機的數據參數設定，將可以透過地面接收站電腦，來監測無人機飛行中的各種姿態參數。

第二階段

1.在完成第一階段的實驗工作後，可獲得完整的四軸無人機的機體結構，第二階段則進行無線傳輸架構設計，確保使操作者的控制指令能正確的傳輸至無人機控制端來進行實驗。

2.將控制指令進行加密運算，本計畫採用 RSA 加密演算法進行設計，並且使加密後的指令，透過無人機控制端的 MCU 晶片進行解密運算得到明文指令，並進行指令確認。

第三階段

1.進行四軸無人機系統機電整合開發，在第二階段所建立的無線傳輸架構以及 RSA 加密演算法，我們使無人機在接受密文指令後，進行解密運算並確認開機指令，能夠遠端開啟無人機系統，並進行資料的可視化，藉以驗證資料的保密性。

2.完成成果報告製作。

第五節 預期效益與對軍事教育改革潛力

5.1 預期完成之工作項目

1.設計並製作完成可以穩定操作的四軸無人機裝置。

2.設置 RSA 加密演算法及可視化設備來驗證與測試。

3.建立四軸無人機系統的無線傳輸架構及機電整合控制。

4.完成遠端無線控制無人機系統實驗，包括資訊的加密性及控制指令的正確性驗證。

5.2 預期成果

1.International conference paper*1。

2.獲得實用化四軸無人機結構、控制裝置及操作特性，包括無線傳輸架設、機體結構架

設、程式設計、資訊加密、資訊解密等技術，以上特性分析可做為學術研究及工程應用之參考。

3.獲得非對稱式加密演算法特性之研究，包含密碼學、可視化技術、機電整合控制及私有密鑰設計、通訊協定設計及開發無人機軍事應用等。

5.3 軍事教育改革潛力

參與人員可獲得非對稱式加密技術、密碼學技術、機電整合技術及四軸無人機機構及資料無線傳輸技術及通訊協定選用方法。

第二章 成果內容：

一、研究成果

在本研究中，我們成功開發了一套創新的無人機安全控制系統。該系統的核心架構包含三個主要部分：雲端操作者端、地面加密端以及無人機驗證端，這三個部分通過精心設計的通信協議和加密機制相互配合，共同構建起一個安全可靠的無人機控制環境。並且依上述的系統架構進行實作，透過 MQTT 傳輸協定方式傳送到雲端網路上的，所以具備裝置接收的功能，例如：可以透過網際網路的傳輸控制訊號，來控制無人機裝置，MQTT 操作介面，如圖9：MQTT 傳輸協定。

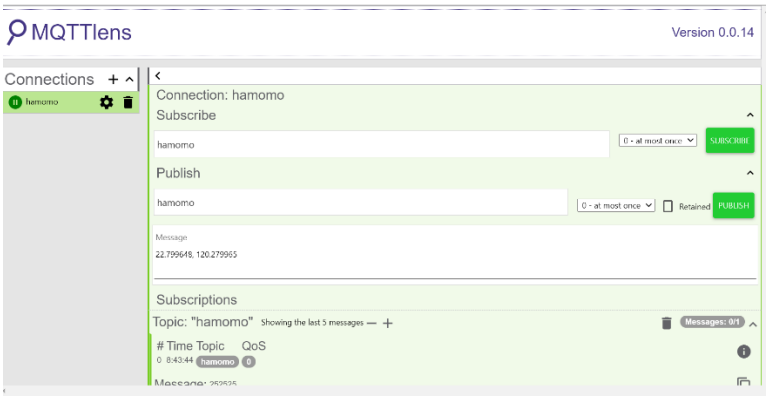

圖10：MQTT 傳輸協定

在雲端操作者端，我們採用了 MQTT 網際網路傳輸協定作為核心通信方式。這使得使用者能夠通過操控主控端電腦，輕鬆設定並發送無人機的控制指令。MQTT 協定的採用不僅確保了通信的穩定性，更帶來了傳輸的優勢，讓系統能夠同時控制無人機裝置，大大提升了系統的實用性和擴展性。

地面加密端的設計中，我們選用了具備 WiFi 連接功能的 ESP32 DVKIT V1 晶片作為核心處理單元，如圖 9 所示。這個部分負責接收來自 MQTT 傳輸協定的控制訊號，並通過 UART 傳輸介面將資料傳送至單晶片進行處理。在這個階段，系統會對控制資訊進行 RSA 加密運算和電子簽章處理，確保資料傳輸的安全性，如圖 10 所示。為了方便觀測和驗證加密過程，我們特別在系統中整合了 LCD 顯示器，這讓實際操作和測試變得更加直觀和便利。

圖 9：ESP32 DVKIT V1

在實際測試中，我們建立了完整的驗證流程。首先確保測試環境具備 WiFi 網路連接，讓 ESP32 能夠順利連接網路並讀取資料。接著，我們逐步驗證了系統接收控制資訊、執行 RSA 加密運算和電子簽章運算，以及透過無線傳輸模組發送加密資訊等關鍵功能。無人機驗證端的設計根據系統架構上的設計。這個部分負責接收加密後的控制訊號，並通過單晶片進行解密和認證。經過處理後的控制指令會通過單晶片的 IO 腳位傳送至無人機飛行控制板，確保無人機能夠接收到安全且正確的控制指令。我們同樣在這個部分整合了 LCD 顯示器，用於即時監控解密運算和電子簽章認證的過程，如圖 11 至圖 14 所示。

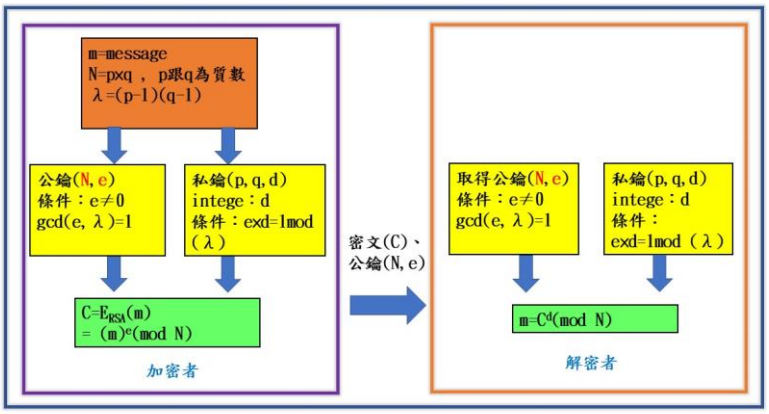

圖 10：RSA 加解密演算法

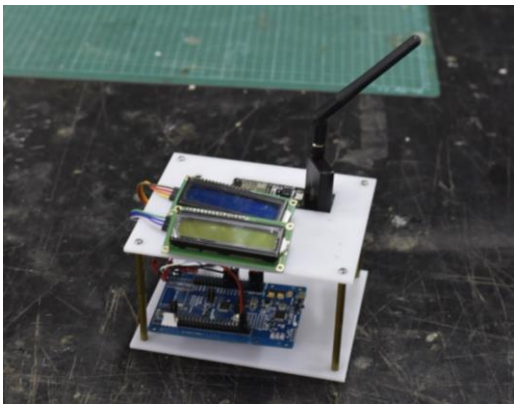

圖 11：地面加密端實作架構

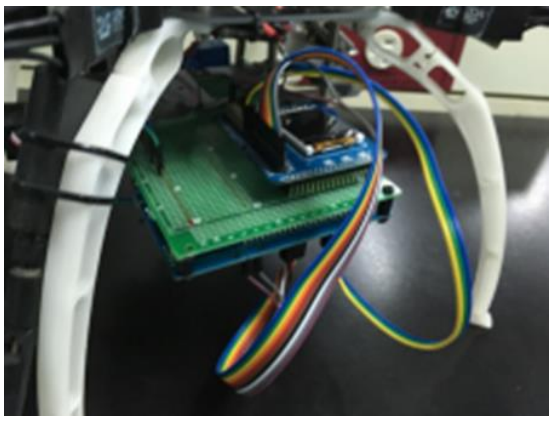

圖 12：整合 MCU 晶片

圖 13：多架無人機端

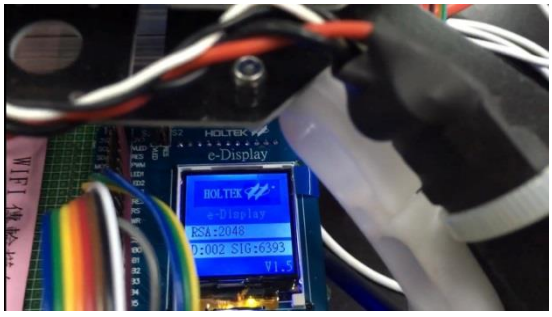

圖 14：密文解密後的資料顯示

二、結論

本研究的主要目標是通過 RSA 加解密演算法和電子簽證方式，為無人機控制系統提供全方位的安全防護。我們的系統成功實現了對控制資訊的雙重保護，有效防止惡意攔截和竊取。系統的一大特色是採用軟體編碼方式實現保護功能，這使得私鑰和公鑰可以靈活更改，大大提高了系統的安全性。即使惡意人士進行長時間的資訊觀察，也難以破解加密的控制指令。經過實際測試和驗證，我們的系統展現出優異的性能和可靠性。無線控制訊號的加密性和正確

性得到充分保證，為無人機的安全操作提供了堅實的技術支撐。這個研究成果不僅解決了當前無人機控制系統面臨的安全挑戰，也為未來相關領域的發展提供了有價值的參考。

三、未來改進方向

基於本研究的成果，我們提出以下幾個可能的改進方向：

1、加密演算法優化：

在現有的 RSA 加密基礎上，可以考慮導入更先進的加密技術，如橢圓曲線密碼學（ECC）。ECC 能提供與 RSA 相同等級的安全性，但所需的密鑰長度更短，運算效率更高，特別適合資源受限的嵌入式系統。

2、通訊協定增強：

可以在 MQTT 協定基礎上增加額外的安全層，如導入 TLS/SSL 加密，或是實作端到端加密機制。同時，可以考慮支援其他通訊協定，提高系統的相容性和適應性。

3、身份認證機制擴展

在現有的電子簽章基礎上，可以導入更完善的身份認證機制，如多因素認證或生物特徵認證，進一步提升系統的安全性。還可以考慮整合區塊鏈技術，實現去中心化的身份驗證和操作記錄。

4、硬體效能提升

考慮採用效能更強的微處理器，以支援更複雜的加密運算和更快的資料處理速度。同時，可以優化電路設計，降低功耗，延長無人機的飛行時間。

5、安全性測試完善

建立更完整的安全性測試框架，包括：定期進行滲透測試及時發現系統漏洞、模擬各種攻擊場景、驗證系統的防禦能力、建立安全性評估指標，量化系統的安全表現。

這些改進方向不僅能夠進一步提升系統的安全性和可靠性，也能為無人機控制系統的發展提供新的思路和可能性，隨著技術的不斷進步，藉由這些改進將能為無人機應用帶來更安全、更高效的操作環境。

參考文獻

[1] Y. Li and C. Tan, A survey of the consensus for multi-agent systems. Systems Science & Control Engineering, 7(1), 468-482, 2019.

[2] R. C. Cavalcante, I. I. Bittencourt, A. P. da Silva, M. Silva, E. Costa, and R. Santos, A survey of security in multi-agent systems. Expert Systems with Applications, 39(5), 4835-4846, 2012.

[3] C. Fontaine and F. Galand, "A Survey of Homomorphic Encryption for Nonspecialists," EURASIP Journal on Information Security, vol. 2007, pp. 1–10, 2007.

[4] R. C. Cavalcante, I. I. Bittencourt, A. P. da Silva, M. Silva, E. Costa, and R. Santos, "A survey of security in multi-agent systems," Expert Systems with Applications, vol. 39, no. 5, pp. 4835–4846, 2012.

[5] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472, 1985.

[6] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes. Springer Verlag Berlin, 1999.

[7] X. Zhou and X. Tang, Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th international forum on strategic technology, Vol. 2, pp. 1118-1121, IEEE, 2011.