穿戴式設備電子健康記錄資訊傳輸安全與隱私

慈濟大學

指導教授：李添福 教授

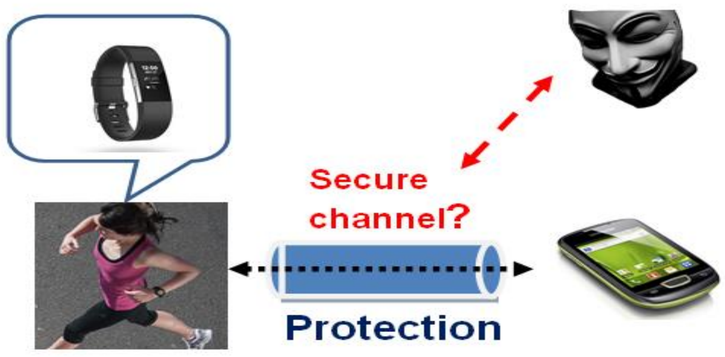
組員：高靖珊、吳偲華、孔廷舜

簡介

利用混沌映射(Chaotic maps)技術發展適用穿戴式設備環境之輕量化運算ID-based(Identity-based)金鑰認證機制，並利用Arduino與感測元件實機模擬。

動機與目的

本計畫希望利用混沌映射技術於效能上優於一般傳統使用模指數運算和橢圓曲線之點乘法運算之密碼系統，導入輕量化運算之加密功能，實作植基於混沌映射技術之金鑰協商機制，以強化穿戴式裝置與可攜式儀器設備之傳輸安全(如圖一)，並與整合物聯網設備中裝載具之安全傳輸協定，提升整體環境之安全性，以確保病患個人隱私及生命安全不受威脅。

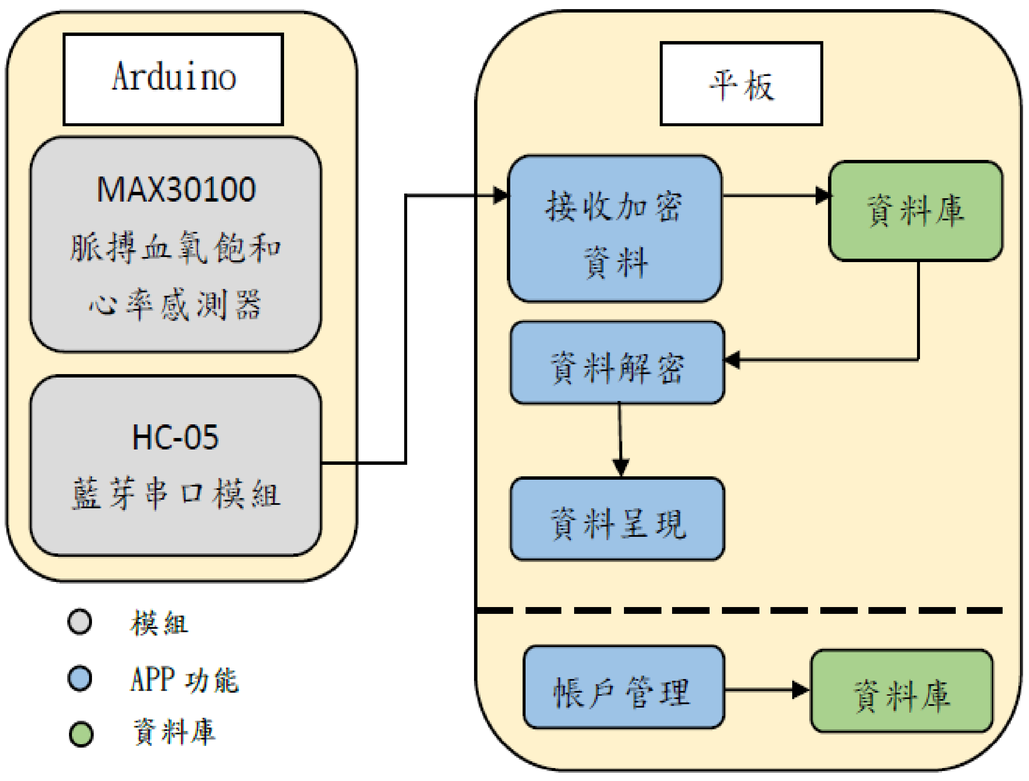


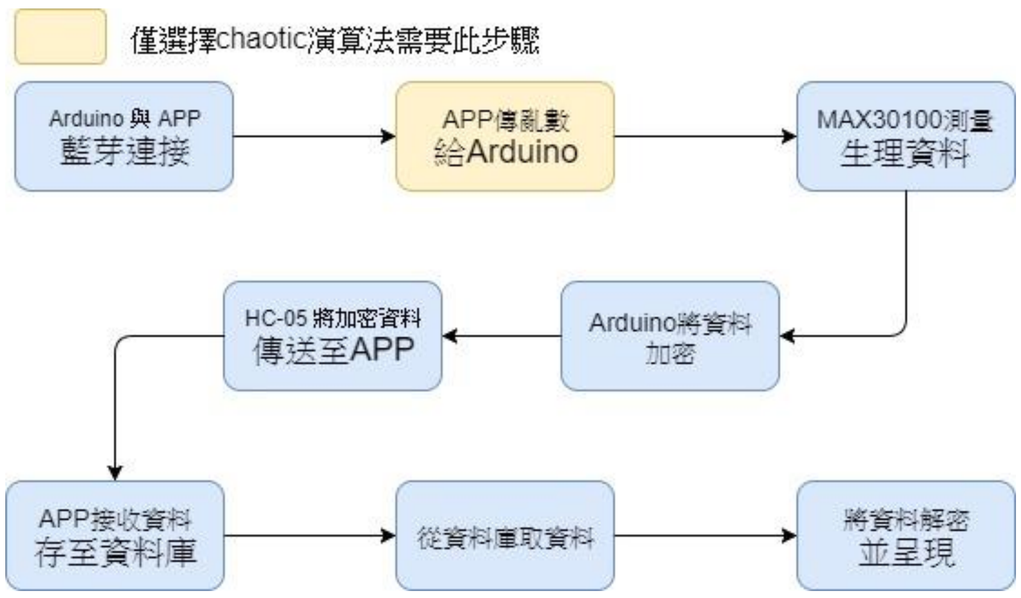
圖一、穿戴式裝置與可攜式儀器設備之健康記錄資訊傳輸安全

開發環境

1. 開發環境： Windows10、SQL server、Android studio2.3、Arduino 1.8.3。
2. 執行平台： PC、行動裝置、Arduino UNO。

系統、功能架構





Arduino

1. 測量生理訊號:
   利用MAX30100測量生理訊號。
2. 生理訊號加密:
   將測得生理訊號在Arduino上進行加密。
3. 加密生理訊號傳輸:
   透過HC-05將加密資料傳輸至平板。

平板:

1. 接收加密生理訊號:
   透過平板藍芽接收加密資料。
2. 資料庫存取:
   平板從資料庫存取加密資料。
3. 帳號管理:
   利用資料庫進行使用者帳號管理。
4. 解密生理訊號:
   取出資料庫加密資料，並於平板端進行解密。
5. 資料呈現:
   資料解密後，顯示於平板端。

系統流程

Step1 使用者註冊基本資料，平板端模擬註冊中心，利用使用者ID，給予secret key
Step2 使用者利用註冊之帳號密碼登入系統，進入加密方法選擇畫面(Diffie-hellman、Chaotic)
Step3 選擇加密演算法
Step4 點選平板端開始測量鈕
Step5 Max30100開始測量生理訊號
Step6 Arduino利用使用者選擇之加密演算法將生理訊號進行加密
Step7 HC-05將加密過後的生理訊號傳送至平板APP
Step8 平板APP將接收到的加密資料存至MSSQL資料庫
Step9 點選平板端停止測量鈕
Step10 平板APP至MSSQL資料庫中取的加密資料
Step11 平板APP利用使用者選擇之解密演算法將生理訊號進行解密
Step12 平板APP呈現解密資料

穿戴式設備電子健康記錄資訊傳輸安全與隱私

慈濟大學

指導教授：李添福 教授

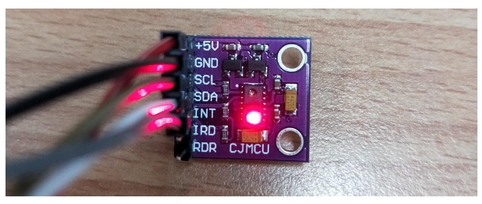
組員：高靖珊、吳偲華、孔廷舜

實作介面呈現

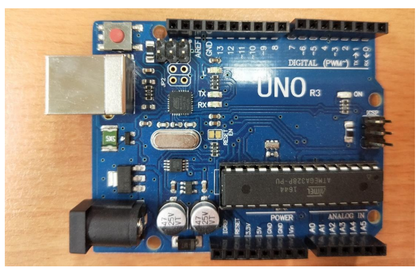
Arduino硬體呈現

MAX30100脈搏血氧飽和心率感測器

利用MX30100脈搏血氧飽和心率感測器測量手指的血氧、心率及溫度再傳至Arduino UNO。



Arduino UNO



利用Arduino UNO取得MAX30100脈搏血氧飽和心率感測器測量之生理訊號，將其訊號進行Diffie-Hellman及Chaotic加密演算法。

選擇 Diffie-hellman ： $A = g^a \bmod p$

$K = B^a \bmod p$

$C = P \text{ XOR } K$

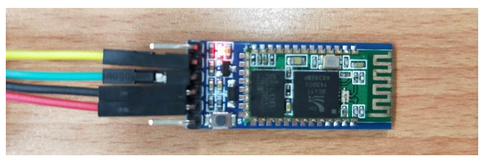
選擇 Chaotic ： $K_{AB} = T_B(SK_A)$

$Key = T_r(K_{AB})$

$C = P \text{ XOR } Key$

HC-05藍芽串口模組

將Arduino UNO加密過後的生理訊號，傳至平板上的App。



APP功能介面呈現

初始頁面

執行App，進入初始頁面，3秒跳轉。

登入頁面

輸入帳號、密碼，驗證成功後，進入選擇頁面。

忘記密碼頁面

當忘記密碼時，可至此頁面尋得密碼。

帳號註冊頁面

新用戶可至此頁面註冊帳號，即可登入使用系統。

選擇加密方式頁面

選擇加密方式後，進入主畫面。

*若選擇Chaotic，平板欲傳一亂數給Arduino。

測量生理訊號頁面

開始測量鈕 － 藍芽正確連接後，點此按鈕，App開始接收Arduino傳的加密生理訊號。
停止測量鈕 － 測量完畢，點此按鈕，停止接收資料。
資料呈現鈕 － 點此按鈕，進入資料檢視頁面。

選擇 Diffie-hellman ： $B = g^b \bmod p$

$K = A^b \bmod p$

$P = C \text{ XOR } K$

選擇 Chaotic ： $K_{AB} = T_A(SK_B)$

$Key = T_r(K_{AB})$

$P = C \text{ XOR } Key$

資料呈現頁面

將加密資料解密，呈現使用者所有生理資料。

未來展望

本專題計畫發展適用穿戴式設備環境之輕量化運算ID based金鑰認證機制，利用混沌映射技術輕量化運算的優點，建構穿戴式設備與訊號接收設備或認證伺服器間的資料傳輸安全管道，強化現行市場上多數穿戴式裝置的安全性，使能兼顧其無線傳輸之安全性與實用性。