Forum: Wireless Product (WiFi, Bluetooth, ..)
Topic: AES128加解密
Subject: Re: AES128加解密
作者: dark
2019年09月29日 22:53:05

引用:

garyyang 寫道：
看網路上介紹藍芽4.0都說有使用AES-128 CCM加密演算法進行封包加密和認證, 請教一下這表示藍芽4.0已經內含AES-128加解密弁　意思是使用藍芽4.0不用額外加解密?

BT晶片都會內建AES block, 因為這是Protocol本身就定義的加密形式, 所以Hw 必備。

但是Hw有不代表你就能去套用, 因為通常BT Stack會把它占住(因為通訊過程中都需要使用AES機制, 只要非Open communication的情況下都要用)

你不是All-in-One的chip就必須在Main chip作解密動作, 不要想在BT chip上做, 因為這還是可以從main chip與BT chip通訊過程中去攔截資料的, 通常BT會做by-pass動作給main chip, 由main chip自行去解密檢查。