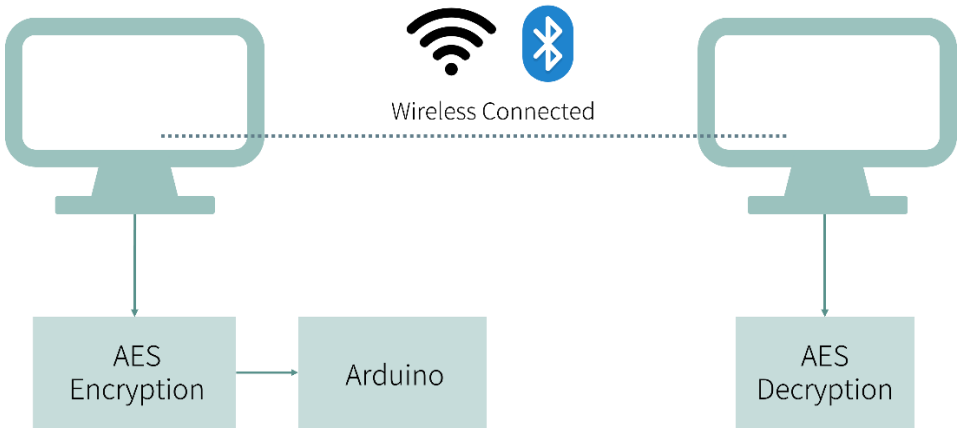
AES 加密系統

指導教授：陳培殷
專題成員：黃律瑛、黃芊
開發工具：Python、C、Arduino、Verilog
測試環境：
Vivado、Xilinx Vitis、Zedboard Zynq-7000

一、簡介：

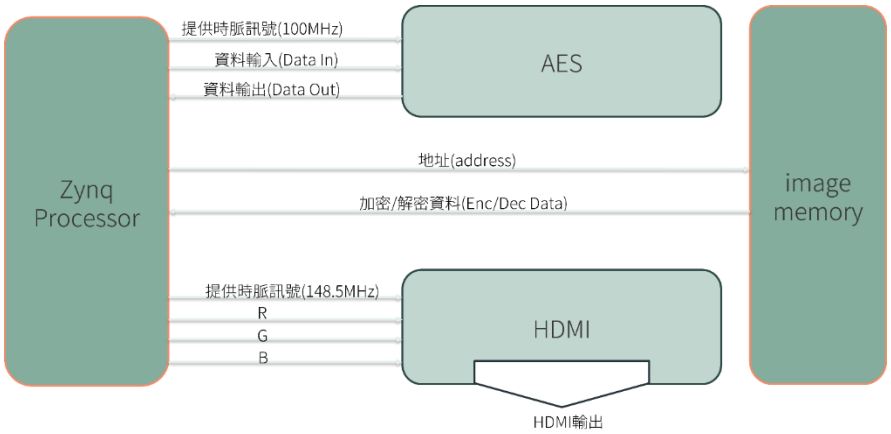
隨著科技的發展，我們即將邁向後量子時代，而最令人擔憂的便是資安問題。量子電腦是量子力學應用於電腦的一種革新工具，具有強大的運算能力，密碼學常見的質因數分解問題、離散對數問題、橢圓曲線問題等等，量子電腦都可以輕易解決，因此現在常用的 RSA 和橢圓曲線加密都將因為量子電腦即將變得不再安全，目前量子電腦的 Shor’ s Algorithm 已經可以攻破 RSA, DSA, ECC 等加密演算法。除此之外，Grover’ s Algorithm 借助量子電腦可以將暴力破解難度從 N 次降為 $N^{1/2}$次嘗試。也就是說，128位元的加密就變成64位元加密的安全性，但是只需要將金鑰長度增為兩倍，即可抵抗這類的攻擊，由此可知，非對稱式加密 (RSA, ECC) 的演算法是需要重新設計的，而對稱式加密 (AES) 演算法僅需增加位元數即可，演算法無須大幅變動。

因此，我們的題目希望能藉由電路實作 AES-256加密，來達到快速、輕量、低功耗的加密。我們利用 Zedboard 模擬加密晶片，將資料在 FPGA 板上加密，再利用無線傳輸將加密資料傳到另一台終端裝置，再利用 FPGA 解密還原資料。而未來希望能直接將晶片(ASIC) 實作在電腦上，在傳出資料之前能快速又低耗能的將資料加密。



圖一：實作之簡易架構圖

二、測試結果



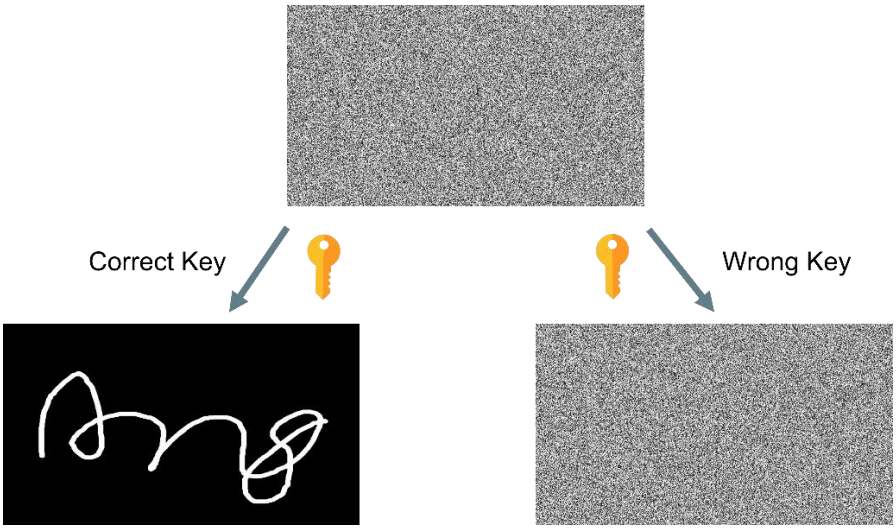
圖二：Block Design Big Picture

我們的題目是以 Verilog 結合 Zedboard Zynq-7000 所實作出來的 AES 加密系統，接下來會用圖二的架構作介紹。

首先，我們藉由讀取照片資料(image memory)，接收使用者想做的功能(加密/解密/結束)，以及使用者所輸入的 key(Data in)，將這些資訊傳送至 AES 進行 AES 演算法。

接下來，加密好的圖片資料會存在 Memory 裡，藉由 Access Memory 將加密好的圖片資料讀取出來，再用 HDMI 的方式呈現出來。(此時為加密的圖片)。下一步，我們會再詢問使用者一次想使用的功能，若使用者想解密，必須輸入前一次所輸入的金鑰進行解密。如同上一步得到功能、金鑰後，將使用者所加密的圖片資料一起傳送到 AES_0進行解密動作。

如果使用者輸入正確的金鑰，將會得到原本那張圖，反之，圖片還會是一片雜訊，最後一樣運用 HDMI 的方式進行輸出。以下是最終呈現出來的結果圖：



圖三：加解密結果