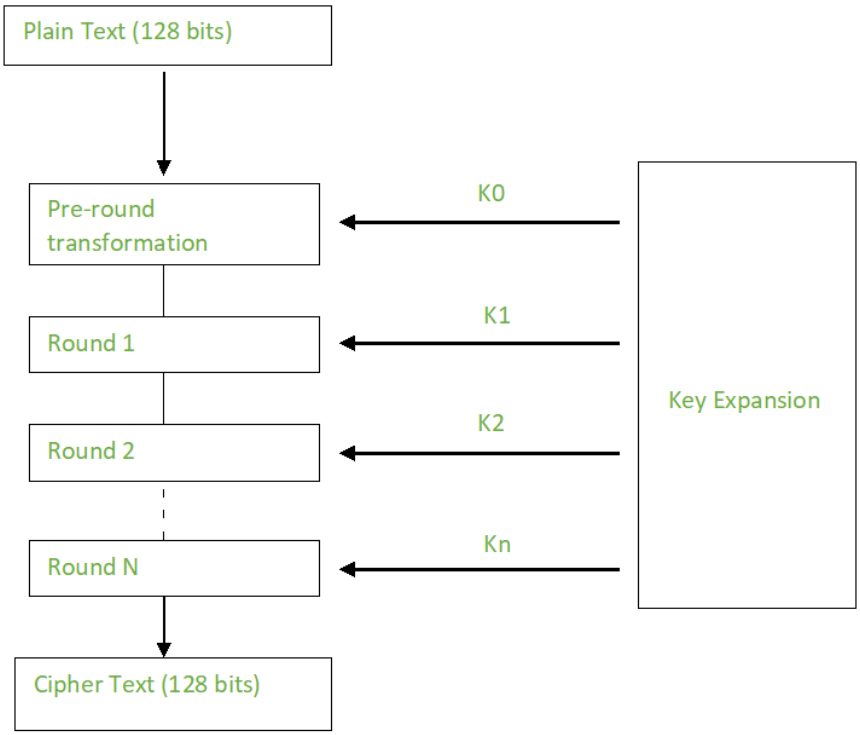
Final project proposal

1. 組員

   111061545 陳揚哲 111061529 周子翔

2. 期末題目

   我們的期末題目是將使用對稱式加密演算法(AES-128)套用至 FPGA 上進行執行，AES-128 的設計上包含 text 和 key 兩部分，原始的 text 會根據原始 key 的進行第一次加密，之後 key 會透過 key expansion 的過程計算出第二把 key，並將其對第一次加密後的 text 進行第二次加密。總共會進行 10 次的加密得到最後的 text 以及 key，因此最後總共使用到 11 把鑰匙(原始 + key expansion 後的 10 把)。解密也是透過相同的方法進行解密，透過反向計算 text 和 key，還原出原始的 text 和 key。



3. 實驗目標

   i. 確認加密和解密的 function 皆正確

   ii. 比較軟體上執行和 FPGA kernel 的運行速度

   iii. 比較 PCIe 的傳輸速度以及實際透過 FPGA 執行的 throughput

4. 實驗設計

   我們將設計兩個 ip，分別是加密以及解密的 ip。

   首先我們會先將 AES-128 加密和解密的程式修改成能符合 HLS 的格式，確定能將其演算法套用至硬體上。

   接著我們會先透過正確對應的未加密 data 和加密 data，以此測試加密和解

密的 function 套用至硬體上都是正確無誤的。
透過 CPU 運算此 function 得到軟體的運算時間以及使用 FPGA 上的 kernel 的硬體運算得到硬體的運算時間，比較軟體和硬體上的加速狀況。
測試完上述的內容後，為了套用至 application 上，我們會使用一個較大的 folder，並對其內部的資料進行加密和解密的運算。理論上，我們認為最主要的 bottleneck 會是 FPGA 上的 PCIe 的傳輸速度，因此最終的 throughput 會接近於 PCIe 的最大傳輸速度。

5. Reference:

   i. https://www.davidwong.fr/blockbreakers/aes_4_key_scheduler.html
   ii. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/