真隨機亂數產生器結合高速影像加密電路

High-Speed Image Encryption Circuit With True Random Number Generator

指導教授：陳培殷、陳朝鈞
專題成員：蔡鎬駿、吳翰宇
開發工具：Verilog、Python、FPGA
測試環境：Vivado、Modelsim

一、簡介：

透過真亂數產生器(TRNG)，及改良過後的 Blowfish 影像加密 (Image Encryption) 技術，去實現一個高速影像加密電路，期望能藉由這項技術，能夠針對重要的影像資料，進行高亂度且快速的加密，去遏止有心人士竊取。

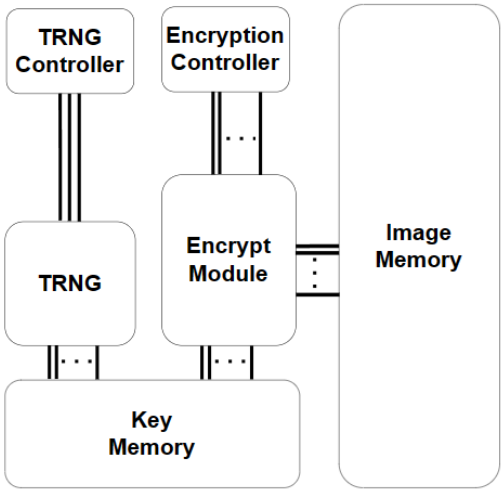
1. 藉由高亂度的亂數獲得更佳的安全性：

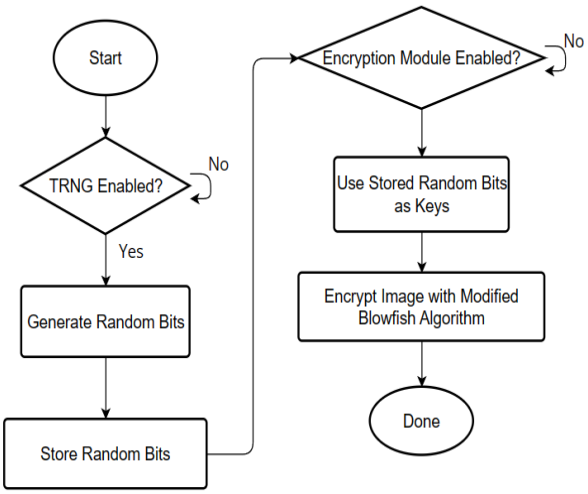
所實作的真亂數產生器(TRNG)能提供高亂度的亂數，去使得密鑰更不容易被破解，透過並結合 Blowfish 演算法，去實現更高安全性的加密電路，附圖為參考資料中，TRNG 所產生的亂數經過測試後的數據。

2.結合更為輕量且高效的 Blowfish 演算法：

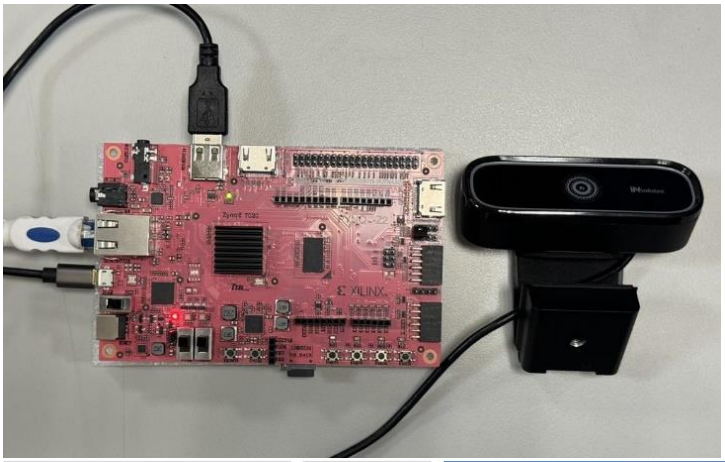
選用改良過後的 Blowfish 演算法，去結合真亂數產生器(TRNG)去提供密鑰，將會比市場常用的其他加密演算法快速且更輕量，同時提供高安全性。

以下為架構圖和運作流程圖：

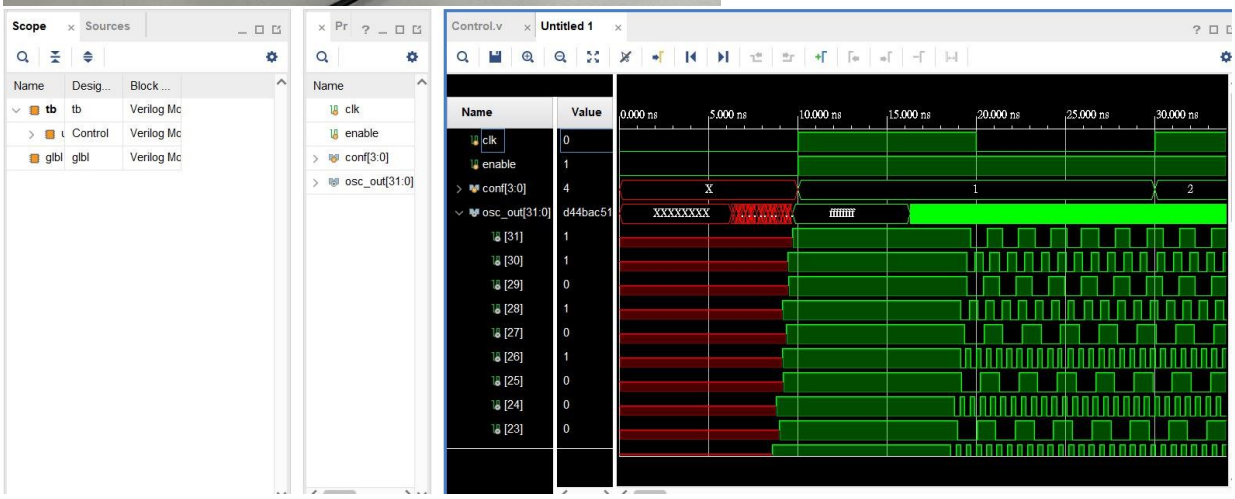




二、測試結果：

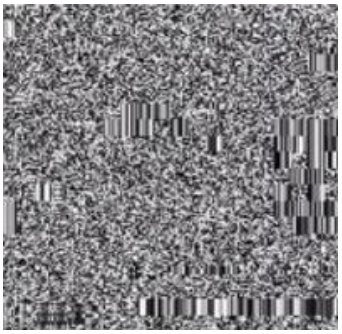


圖一：
選用 FPGA device(Xilinx AUP PYNQ-Z2)來實作高效率影像加密加速器，並透過 V12 網路視訊攝影機(鏡頭：2P2G 定焦/直徑8m，尺寸：94x80x38 mm)進行拍攝，將拍攝完的影像再傳回電路去加密處理。



圖二：透過軟體 Vivado 搭配 ILA 進行模擬，完成真亂數產生器(TRNG)，附圖為透過 Waveform 產生亂數(在不同時間產生0和1輸出)，作為密鑰去結合改良過後的 Blowfish 演算法去進行加密。

圖三：拍攝照片



圖四：加密後的照片

圖五：解密後的原圖

使用高速影像加密電路，並針對 V12 網路視訊攝影機所拍攝的照片，進行上述的加密步驟後，可得到圖四中的 Encrypted Image，成功加密我們所要保護的重要影像，再依照密鑰反向進行解密後，即可將原本的拍攝照片還原。