TPM2.0 在 Rpi2 上的效能測試

指導老師：鄭仁亮教授
組員名單：陳韋諭、吳岱燁、張迺湘

在科技發展迅速的時代，資訊安全越顯重要，可信平台模組(Trusted Platform Module ,TPM)是資訊安全的最後一道防線。業界目前提供硬體及韌體的 TPM 版本，前者以 ARM 為代表後者以英飛凌為代表。

本專題將 TPM2.0模擬器安裝在 Raspberry Pi 2執行，並進行五種基準命令效能測試，將結果與 fTPM(韌體 TPM)及 dTPM(硬體 TPM)做比較。

最後測試結果 sTPM(軟體 TPM)效能相較兩者為低，本專題首次將 TPM2.0成功安裝在 Raspberry Pi 2上，在安裝及指令測試過程中可以藉由此架構去分析 bytestream 和硬體 TPM 去做驗證，利於未來 TPM2.0系統晶片的開發。