**PUF裝置於健康保健資訊資料庫之存取控制**

指導老師：李添福教授

組員名單：徐俊瑋、王郁翔、黃韋傑

近幾年來輕量化運算技術是未來資訊科技的趨勢，相關的研究技術應用於電子健康紀錄與電子病歷，多僅考慮使用者相互認證與資料傳輸機密性，較少研究探討健康保健資訊資料庫存取控制。此外，大多數研究仍仰賴於耗時的模指數運算、橢圓曲線運算之簽章與加密技術，較少研究能完整考慮安全特性下發展輕量化運算健康保健資訊資料庫存取控制之認證機制。Physically Unclonable Functions(PUF)裝置是基於在半導體製造過程中自然發生的獨特物理變化，產生出唯一的識別性與不可預測性，應用於認證加密機制中，在效能上有著重大的改進。本專題針對健康保健資訊資料庫之隱私保護、授權與存取控制等特性，進行更深入探討與分析，並利用PUF技術設計一個安全有效率之於健康保健資訊資料庫之存取控制機制。所提存取控制機制不僅提升病患病歷的隱私性與安全性，使得整個醫療流程更有效率。