植基於物理不可複製函數與區塊鏈技術之電子病歷簽章

指導老師:李添福 教授

組員名單: 林毓文,林子晴,陳敬迪,丘宸安

電子簽章技術提供電子病歷與醫療影像病歷認證、不可偽冒性、不可否認性等功能。現階段電子病歷與醫療影像病歷簽章，含RSA 或 ElGamal 簽章，仍須仰賴於耗時之模指數運算。本專題計畫希望用物理不可複製函數(Physically Unclonable Functions, PUF)技術與區塊鏈技術發展適用於電子病歷與醫療影像病歷之簽章機制。所發展之機制中，利用 PUF 其基於在自製過程中自然發生的獨特變化及施加的物理訊號來產生其獨有的回應，利用每個挑戰(Challenge)只會有一個對應的回應(Response)值之特性作為其識別碼及認證金鑰；並利用區塊鏈技術對於交易資訊進行管控，透過區塊鏈資料的不可竄改性，確保交易訊息的安全、匿名性，讓使用者在交易時，個人資訊能更安全以及資訊公開透明與可回溯。希望藉由本專題計畫所發展電子病歷簽章，除了達到電子病歷簽章應具備之認證、不可偽冒性與不可否認性外，並能提升數位簽章的效率。