



### 摘要

本專題的主要目的是在實作一個投票系統。大部分的投票系統講求方便使用與快速設計，採取了匿名投票甚至不記名投票的方式來進行，但是這樣也造成了有心人士的灌票與重複投票。另一類的投票雖然在投票時會要求填上姓名與個人資料，但是仍然無法有效防範假冒他人資料或輸入虛假資料的情形。因此我們設計的投票系統將使用數位簽章的特性與技術，讓投票者的身份只能與他本人連結，並且投票的內容不會被他人惡意竄改，使投票結果更加的正確公正。

若雜湊值相同無誤，接收方可認為資料沒有經過竄改，同時也證明了接收方使用之公鑰與傳送方的私鑰是同一對的；反之則表示資料可能已遭到竄改，或其來源並不正確。

在投票系統中，我們可以應用數位簽章，將選票的雜湊值與簽章同時發送，以確保其不被竄改、確實為本人發出的；同時由於選票經過雜湊化，也可避免選票所投的對象被第三者知道。

### 成果

本系統能發揮以下功能，使投票公平：

1. 安全：透過數位簽章，投票者投出的選票不會遭到竄改。
2. 保密：透過密碼雜湊，第三者無法得知某人把票投給了誰。
3. 公平：一人一票，投票者不可重複投票。
4. 可驗證：若使用者認為有需要，可進行驗票。

### 研究方法

數位簽章應用了非對稱式加密，用來驗證所接收的資料是否遭到竄改，以及發送者是否無誤，我們以傳送方、接收方兩邊來探討其流程：

