分組名單(不足5個人空著就好):

姓名	學號
陳以晴	111550178
蔡昀錚	111550035
莊婷馨	111550057
謝詠晴	111550113
鄭芯薇	111550064

1. **Name of the paper:**
   Civitas: Toward a Secure Voting System
   Michael R. Clarkson Stephen Chong Andrew C. Myers, Department of Computer Science, Cornell University

2. **Summary:**
   Civitas 是一個具有抗強制性(Coercion Resistance)和投票者驗證性(Verifiability),並適用於遠端的電子投票系統。本文首先描述了Civitas的目的、設計和實施流程,再通過安全證明(Security proofs)和安全信息流(Security information flow)確保設計與實現的可靠性,最後通過實驗結果,評估這個系統在安全性、時間和成本上的權衡。

   傳統的投票假設一切都受到可信的人工監督,然而這在社會中並無法被完全確保,且傳統投票也無法同時保證誠實性(Integrity)和機密性(Confidentiality)。故隨著遠端投票的需求日益擴增,如何架構安全的系統具有重要意義。本文為此設計 Civitas 選票系統,希望解決現有投票系統的主要問題,包含投票時誠實性和機密性的矛盾、對投票過程的信任度不足、匿名度過低等等問題。

   文章中將投票過程分為設置、投票、計票三個部分,討論每個部分如何同時保證完整性與安全性,以及其所利用到的不同算法與加密方法。在設置階段,使用 RSA 公鑰以及 El Gamal Encryption,來提供身份認證及訊息加密驗證等等功能;接者,在投票階段,選民將加密的私人憑證和投票選項發佈到投票箱,並附帶零知識證明(zero knowledge),確保投票的匿名性與憑證的有效性。最後在計票階段,在監督者發布簽名後,清點計票箱(ballot boxes)中有效的票數,並使用混合網路(mixed network)確保身分保密性,最後使用純文本等價測試(PET)判斷是否有重復或無效的憑證,此過程的計算需求很高,因此較為耗時。

   筆者討論了 Civitas 實現的挑戰及可擴展性,如投票證明的效率和選票匿名化處理的複雜性。此外還探討了實際部署 Civitas 的潛在成本,以及進行了一系列的評估實驗,來展示其在大規模選舉中的可行性。

   總體而言,Civitas 為電子投票系統提供了一個新的視角,特別是在提高安全性、保密性和用戶信任度方面,並且嚴謹地證明了系統的安全性,對於未來電子投票技術的發展提供新的發展可能。

3. Strength(s) of the paper:

1. 完善的架構設計
   本論文介紹 Civitas 的運作方式和各個組成零件, 由大致流程說起, 再到假設環境以及實作細節, 最後是實驗結果, 有助於閱讀者由淺入深的理解此系統。
2. 創新性
   筆者提出一個非常創新的網路投票系統, 能夠同時提供隱私保護以及可驗證性, 不僅現行方法(線下投票)無法同時做到, 過去也未曾有類似做法。
3. 密碼學技術應用
   筆者在 Section 5 中, 具體說明該使用哪種密碼學技術實現系統的功能, 包括 RSA public keys, El Gamal encryption (Homomorphic Encryption), Mixed Network 等, 且流程分類清晰, 十分易於閱讀。
4. 實現與評估
   實驗應用於 Jif 中, 並評估該系統的可擴展性、效率和安全性。
5. 簡明的表格
   將實驗所得數據製表呈現, 圖示讓閱讀者更易於瞭解數據趨勢。

4. Weakness(es) of the paper:

1. 缺乏可實用性與可部署性
   雖然文獻中顯示Civitas系統已經擁有強大的安全性, 但他尚未能應用在國家正式的選舉當中, 例如縣市首長選舉或總統大選, 這使得結論中提到的普遍性和實用性有待商榷。
2. 太過理想化
   雖然從理論層面來看Citivas已經有強大的安全性與可靠性, 但他還沒有在大規模的實境中被測試和驗證, 也尚未應用在實際的選舉上, 因此有些潛在的問題無法在文獻中被充分探討。
3. 過度信任脅迫防禦
   Civitas系統強調抗脅迫性, 但是當面對高技術性或擁有許多資源的網路攻擊者時, 在沒有面對面監督的遠程投票情況下未必可以完整實現這個性質。
4. 系統運作流程過於複雜
   雖然複雜的算法與加密法可以高程度地保證系統的安全性, 但同時也造成選民在投票時的不方便, 這可能導致此系統無法有效率且廣泛地運用於大型投票。
5. 忽略實際使用方法
   本論文未探討遠程投票系統在實際應用時的用戶界面設計與操作流程, 而是集中討論了選民身份驗證與加密技術的具體細節, 忽略了如何提升用戶體驗與操作便利性的重要性。

5. Your own reflection, which can include but not limited to:

A. What did you learn from this paper?

(1) 加密組件:在第五段落 Cryptographic components 中提及 Civatus 使用了許多加密組件, 包含數字簽名、零知識證明以及非交互式的 Fiat-Shamir heuristic 的概念。其中零知識證明是指:向對方證明自己擁有某一情報, 卻又能達成不透漏該情報內容, 用於確保協議可誠實執行而不洩露任何額外信息。而在此篇論文中, 透過 Fiat-Shamir Heuristic(啓發式)變為非交互

式, 即只需要一方提供證明, 另一方則可以單獨驗證, 因此可減少通訊的開銷需求。

(2) Civitas 系統階段:我們學習到 Civitas 遠程投票系統的設計, 例如將系統設置、投票以及清點來分析, 而在各階段的實施面上, 需透過一連串的步驟:公布 RSA 及選民公鑰、獲取私人憑證、建立會話鑰匙以及確認是否有重複及無效憑證, 在過程中, 也運用到如 El Gamal 加密方案、混合網路和純文本等價測試(PET)等技術。實施和評估過程中, 要如何兼顧保護安全、透明及抗強迫性是一大挑戰。本論文中不僅探討了電子投票中的技術挑戰, 包括加密組件的使用、可擴展性和安全性, 還強調了需要應對的社會挑戰, 如公眾對投票系統中密碼學的接受程度、遠程電子投票的可訪問性以及對選舉程序的現實世界攻擊。

B. How would you improve or extend the work if you were the author?

(1) 此系統已有完整的架構, 因此我們會更朝向用戶友好性(user-friendly)的層面, 思考如何使投票系統的操作或是介面更加利於使用者使用, 或是能適用於更廣泛的選民。

(2) 可以將如何實現遠端投票的整體方法敘述得更加具體與完整, 例如從初期階段的投票人身份驗證、投票網站架設以及如何篩選值得信賴的登記櫃員, 到後期的投票界面登入資訊(投票時須提供投票人的哪些基本資料).....等。

(3) 如何處理應用層面的拒絕服務攻擊, 以及遮斷網路、木馬侵害用戶電腦等等, 另外還有選民對電腦的存取需求

(4) 當出現網路斷訊, 服務器崩潰等等致使選民目標與實際結果不合時如何驗證、復原或解決。

C. What are the unsolved questions that you want to investigate?

(1) 對於選民可能會嘗試出售他們的私人註冊密鑰加以管制, 例如將其與其他加密(如指紋, 虹膜, 身分證等)綜合。

(2) 在成本計算中, 僅以機器能耗等等成本與傳統人力成本比較, 但文章所述之實際流程中提及實體登記部分, 此部分成本無舉出

(3) UI 實際應用介面:由於此系統複雜的流程與算法, 要設計出簡潔易懂的介面才能增加實用性, 但本文中並未提到這點。

(4) 網路安全性:本文並未提到如何有效防範駭客入侵等情況, 實作方面上仍需要相關技術支持。

(5) 因任何原因導致的紀錄票數之檔案崩潰時如何回復。

D. What are the broader impacts of this proposed technology?

(1) 增加投票參與度:透過更加安全且支持遠端投票的系統, 將提供遠距離選民的便利性, 進而提高參與投票之比率。

(2) 將會影響相關法律的制定:透過網路投票有可能造成技術的濫用或安全性的疑慮, 因此需要新的法律和政策來規範其應用來保護選民的隱私。

(3) 提高投票的公平公正性:由於此系統提供了一個能防範強制投票等現象的環境, 因此可以提供選民更好的投票自主權。

E. Else?

我們對其創新的技術細節與設計印象深刻, 尤其是在提升投票的安全性和保護選民隱私方面的潛力。然而, 我們認為此系統距離被廣泛使用還有很多困難要克服, 包括系統的性可能對普通選民的可接受性造成影響, 以及在實際部署中需要大量技術支持和增加的成本。因此, 推動這類技術的廣泛接受和應用, 需要多方維護, 以確保技術的正面影響得以實現, 同時也謹慎處理相關的風險。