Critique 2

姓名	學號
朱驛庭	111550093
王睿宇	111550085
邱振源	111550100
黃佑得	111550160
陳 燁	111550124

Name of the paper

> Civitas: Toward a Secure Voting System

Summary

這篇文章藉由設計了一個名為Civitas的系統，對建立一個安全的電子投票系統領域，進行了一個全面而廣泛的探索。科技日新月異，電子投票也不再只是天方夜譚，當科技與社會的各個層面交織在一起之後，如果要採納電子投票，那確保系統的安全性和完整性至關重要。因此作者設計了Civitas，不僅能促進高效投票，還能防範竄改，和脅迫等等潛在威脅。

Civitas的核心是將加密技術、透明性和可驗證性原則相互融合。與傳統的紙本投票方法不同，電子投票系統提升了效率然而，它也帶來了每張選票的可信度和安全性的全新挑戰。作者提出Civitas，為調和這些相互衝突的需求的開創性解決方案，提供一個強大的框架來平衡隱私需求與可信度的必要性。

Civitas的核心思想之一是致力於選票保密。在任何民主選舉中，個人選票都是保密而平等的，藉由不記名投票的方式，確保公民可以表達自己的偏好的候選人而不必擔心遭到報復。 然而，在電子投票環境中實現這種保密性並非易事。 Civitas利用先進的加密協議對選票進行加密和匿名化，從而保護選民的隱私，同時仍能準確地統計結果。

此外，Civitas非常重視可驗證性，並認知到對選舉過程的信任，取決於利益相關者獨立驗證結果完整性的能力。 透過使用加密證明和公共審核機制，該系統使任何人都可以審查選舉的進行，並驗證結果是否準確反映了選民的集體意願。這種透明度不僅增強了人們對選舉過程的信心，而且對潛在的買票行為起到了威懾作用。

除了解決電子投票系統安全的技術挑戰外，Civitas還面臨到如何實現的問題。因為任何可行的解決方案都必須在現實世界基礎設施和營運需求的限制範圍內可行。因此，他們提出了一種務實的方法，優先考慮簡單性、可擴展性以及與現有選舉系統的兼容性。透過採納並遵守這些原則，Civitas弭平了密碼學研究的理論與選舉背景下的實際部署之間的差距。

Civitas的重要性不僅在於其技術創新，同時，它將民主原則與法治社會推向一個全新的境界。在一個對選舉信用度和國際上的全里干涉充滿擔憂的時代，對值得信賴的電子投票系統的需求時十分迫切的。透過提供安全、透明和可驗證的選舉系統，Civitas為解決這樣的現況提出了一種解決方案。

總之，Civitas: Toward a Secure Voting System為電子投票的未來提出了令人期待的美好憧憬。透過綜合加密原則、透明機制和實際考慮，Civitas 為建立安全的選舉系統提供了強而有力的基礎。

Strengths of the paper

首先，論文的結構井然有序，使我們能夠循序漸進地理解 Civitas 系統的架構與運作原理。從系統的概念設計到具體的實施細節，這篇論文都進行了細致的說明。透過清晰的技術描述和有效運用圖表和模型，論文讓讀者易於理解複雜的加密方法和投票流程，以及這些技術是如何整合來保證投票的隱私和完整性的。

在安全分析方面，作者不僅描述了系統的基本安全特性，如抗脅迫性和可驗證性，更深入探討了在面對現實世界威脅時，這些安全特性是如何被維持的。論文明確了多項安全假設，並根據這些假設進行了嚴密的安全證明，展示了 Civitas 如何抵抗不同的攻擊。此外，對潛在的安全風險進行了詳細的分析，並提出了相應的風險對策，這些都表明了作者對系統安全性的全面考量和對策的深思熟慮，另外這篇論文還提供了數學證明來支持其安全性主張，這不僅增加了論文的技術深度，也為該投票系統的安全性提供了堅實的理論基礎。

通過這種系統性的研究和細致的描述，論文不僅提供了一個理論上可行的選票系統設計，還展示了如何在實際應用中實現高度的安全性和可操作性。這使得 Civitas 不僅是一個理論上的創新，更是向實際應用靠近的一大步，為未來的電子投票系統的發展提供了寶貴的參考和基礎。

此外這篇文章不僅關注技術的實現，還特別強調了系統在不同環境下的適應性，包括在無法確保投票場所受監督的情況下如何保持系統的安全性。這顯示了 Civitas 在設計時考慮到了廣泛的使用場景，從而增強了其在實際應用中的可行性和廣泛性。

Weaknesses of the paper

Civitas投票系統的具體實現涉及當該系統在實際選舉環境中部署時會遇到的諸多困難。這些挑戰中，保證所有投票客戶端的安全性尤其重要，因為在實際情況中，要保證每位選民的裝置免受網絡威脅幾乎是不可能的。這種安全性的假設增加了系統被破壞的風險，可能導致選票被操縱或隱私被侵犯。此外，Civitas系統本身的複雜性可能對不熟悉技術的普通選民構成挑戰，他們需要管理多重認證，甚至可能需要生成假認證以抵抗脅迫，這需要在不損害安全功能的前提下確保用戶友好的體驗。系統還要求選民與註冊服務員之間的通信頻道必須是安全且無法竊聽的，保證這一點在不同的網絡環境中極具挑戰性。除此之外，Civitas需能抵抗潛在的拒絕服務（DoS）攻擊，這種攻擊可能針對選舉當局或基礎設施，目的是延遲或破壞選舉進程。此外，系統對安全且匿名的通信頻道的依賴在現實操作中也難以實現，尤其是面對可能控制網絡基礎設施的先進對手時。最後，要獲得公眾對使用複雜密碼協議的電子投票系統的信任是一個重大挑戰，這需要透明度、可驗證性和易於理解等關饒因素共同作用，這些是確保選民和利益相關者對系統既安全又公平持有信心的關鍵要素。

Reflection

在這篇論文中，作者展示給我們看了一篇完整有關投票系統的論文，包含了Security Model的建立、參與投票系統的人的身分、投票的流程(Setup phase、Voting phase)、Threat model跟對應的安全性分析、以及這個投票系統背後的理論支持，雖然這篇論文沒給Preliminaries，讓我們讀的時候需要先理解一下某些資安的基本名詞，但是作者都有放相關的reference，讓讀者可以自行參閱，這點之後如果我們自己寫論文要多注意可以補這些東西。

此外，透過這篇論文，我們也發現要提出一個非常安全的資安模型不是一件容易的事，以Civitas為例，雖然他已經在怎麼保護voter、怎麼架好voting system，但是實際上他還是有很多的Trust assumption，舉例來說，Trust Assumption 4說 *The channels on which voters cast their votes are anonymous*，或許可以利用一些資安相關的技術來確保這件事情成立，但是可能會實作複雜，我們認為說作者會假設這個條件原因是這個假設並不在這篇論文主要討論的目標(論文主旨是提出了一個安全的投票系統)，為了加速研究的進行，作者選擇假設這格條件直接成立，這個方法之後我們如果做資安或是其他領域的論文也可以用，不必為了偏離主旨的事情而拖到研究進度。

最後，我們認為這篇論文的完整性非常出色。作者不僅提供了大量相關研究和程式碼，更進一步評估了Civitas在現實世界中的潛在效益。這種評估不僅加強了論文的實用性，還使得讀者能夠更清晰地了解該系統在真實環境中的影響。除了深入探討理論方面，這項實際效益的估算使得論文更具廣泛的應用價值，同時也提供了實踐中的指導和啟發。