分組名單（不足 5 個人空著就好）:

姓名	學號
施柏江	110550108
王振倫	110550068
林英碩	110550117
呂偉祥	110550115

1. Name of the paper:

   Civitas: Toward a Secure Voting System

2. Summary:

   The paper addresses the challenge of designing a secure electronic voting system that ensures voter privacy, prevents tampering with votes, and provides verifiability. With the increasing reliance on electronic systems for voting, it's essential to develop solutions that can guarantee the confidentiality and accuracy of votes while allowing for transparent verification processes.

   It also proposes the Civitas system, which employs cryptographic techniques and robust system design principles to tackle the challenges. It utilizes encryption to protect voter privacy, digital signatures for verifying the authenticity of ballots, and distributed architecture to prevent single points of failure or manipulation.

   The work demonstrates the feasibility of building a secure electronic voting system through the Civitas framework. By combining cryptographic methods with careful system design, the paper suggests that it is possible to create a voting system that maintains voter privacy, ensures ballot integrity, and enables verifiability, thus addressing critical concerns in electoral processes.

3. Strength(s) of the paper:

   Firstly, it offers a comprehensive approach to tackling security issues in electronic voting, which is crucial for maintaining trust in democratic processes and ensuring the integrity of election results. The implementation of Civitas utilizes information-flow security analysis, enhancing the security of the system and protecting voter confidentiality.

   Secondly, it provides detailed explanations of the cryptographic techniques and distributed protocols used in the Civitas system, making it accessible for

readers interested in understanding the technical aspects.

Thirdly, the paper provides experimental results that offer a quantitative evaluation of the tradeoffs between time, cost, and security, providing valuable insights for decision-making. It also explores trust assumptions related to in-person registration and availability, addressing key aspects of trust in the voting system.

Additionally, the paper presents a thorough analysis of potential threats to the voting system and proposes effective countermeasures to mitigate these risks. Overall, it contributes valuable insights to the field of secure electronic voting systems and technical advancements in secure registration protocols and scalable vote storage systems.

4. Weakness(es) of the paper

One potential weakness of the paper is that it may be challenging for readers without a strong background in computer science or cryptography to fully understand the technical details. Providing more intuitive descriptions or illustrations could help make the content more accessible to readers.

Another potential weakness is that while the proposed Civitas system addresses many security concerns, it's important to note that no voting system is entirely immune to vulnerabilities or attacks. Further testing and real-world implementation would be necessary to validate the effectiveness and practicality of the proposed solution.

Also, this paper acknowledges that Civitas is not yet suitable for deployment in national elections, indicating potential limitations in scalability or real-world applicability. There is also an open problem left in the paper about the electronic voting systems, such as transparency of voter and vulnerability to malware, suggesting ongoing challenges in ensuring the security and integrity of electronic voting systems.

Overall, even though there are some flaws in this paper, its innovative approach of the electronic voting system is a strong security foundation, there is still space for further exploration and improvement.

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

A. What did you learn from this paper?

From this paper, we learned something about the importance of security in electronic voting systems and how cryptographic techniques can be used to protect the integrity and privacy of the voting process. It also highlights the complexity of designing secure voting systems and the need for thorough analysis and testing to identify and address potential vulnerabilities. Overall, the paper provides valuable insights into the challenges and solutions involved in creating trustworthy electronic voting systems.

Additionally, we also learned that the paper successfully demonstrates the feasibility of constructing a secure electronic voting system using the Civatas framework. It represents a significant advancement in the field of security. The insights we gained from this paper can guide the future development and implementation.

Moreover, the system's adaptability is a proof to its creators' creativity. The flexibility of satisfying different voting requirements allows the system to address the unique challenges which are faced in various election scenarios. This ensures that the security and the privacy preserving methods remain effective. Their creativity helps us see that we may have a safe electronic voting system someday in Taiwan.

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

If we were the author, we might consider conducting further real-world testing and simulations to assess the practicality and scalability of the Civitas system. For example, we can conduct a far smaller experiment in our committee member election in our school to verify the practicality of the electronic voting system. By a real-world experiment we can collect the advice of people to see whether the electronic voting system is truly needed or the difficulties of implementing it.

Additionally, we would explore ways to make the system more user-friendly and accessible to a wider range of voters, perhaps by designing intuitive user interfaces or incorporating mobile voting options. Moreover, continuous monitoring and updates would be essential to adapt to emerging security threats and ensure the long-term effectiveness of the voting system.

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

Some unsolved questions we'd like to explore include how to improve voter authentication methods to prevent fraud, how to balance transparency with voter privacy in electronic voting systems, and how to effectively mitigate potential cyberattacks targeting the integrity of the voting process.

Additionally, we'd be interested in researching ways to enhance accessibility and inclusivity in electronic voting to ensure that all eligible voters can participate easily and securely. Experience and convenience are also an important part of the election process, it can significantly influence the willingness of people to use the remote voting system.

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

The proposed technology for secure electronic voting, like Civitas, could have significant broader impacts on democracy elections. It could increase voter turnout by providing more convenient and accessible voting options, particularly for people with mobility issues or those living in remote areas.

Additionally, it could enhance the integrity of elections by reducing the risk of tampering or manipulation of ballots if we could ensure security in the electoral process. Moreover, it might inspire trust and confidence in the electoral process, fostering a stronger sense of civic engagement and participation in democratic societies.

Lastly, if it could also include a friendly mobile app for voting, this app could make the voting process efficient and accessible to a wider range of voters, especially younger generations like us. With just a few taps on our smartphones, voters could securely cast their ballots from anywhere, increasing participation and engagement in elections. This addition could change the way we vote, making it more convenient for everyone in Taiwan.