Critique 2

Department :資工系　　Student ID : 109550198　　Name : 卜銳凱

“Civitas: Toward a Secure Voting System” Michael R. Clarkson, Stephen Chong, and Andrew C. Myers from the Department of Computer Science at Cornell University.

Summary:

The paper "Civitas: Toward a Secure Voting System" reports the design and implementation of Civitas, the first electronic voting system that is coercion-resistant, universally and voter verifiable, and capable of distant voting. In contrast to commercial electronic voting systems, Civitas includes strong security proofs in the design, ensuring secure information flows during implementation.

Civitas is based on a cryptographic voting mechanism that ensures the integrity and confidentiality of votes. Integrity is achieved through means that ensure that all interested parties can tell if the votes are correctly counted and that any other attempt to corrupt the election is detected. Cryptographic techniques ensure voter anonymity and that vote selling or coercion is not possible; this maintains the confidentiality of the election.

Civitas is designed in a distributed manner, meaning confidence is distributed across several authorities instead of being centralized. This makes the possibility of a single point of failure endangering the election much lower. A variety of cryptographic components is utilized in Civitas, including secure registration, anonymous voting, and a mix network for secure vote tabulation.

The results of experimentation reported in the paper illustrate the trade-off between security, cost, and time in computing, and it shows that Civitas can improve security at a reasonable cost. It is not suitable for national election use yet, but it is a large step toward the desired electronic voting.

Strength(s) of the paper:

The paper "Civitas: Toward a Secure Voting System" reveals several major features that make it, in many ways, an improvement of its contribution to the domain of electronic voting systems.

Civitas achieves strong security mechanisms that make it overcome major failures in the state of the art on electronic voting systems. The architecture makes the system coercion-resistant,

meaning that the voter has no way of being forced to vote a certain way. This is very important in protecting the freedom and secrecy of voters' decisions.
Comprehensive Verification: The system supports both universal and individual voter verifiability, assuring the integrity of the voting process. The voter can ensure that his/her vote has been accounted for, and any observer can have it confirmed that all votes have been accounted for as cast. This helps in increasing the level of trust in the electoral process because it makes it more transparent and auditable.
Civitas is designed to allow for remote voting, which becomes increasingly important in a society where ease and accessibility are paramount. Such an option will enable elections to take place in a variety of locations while ensuring security and, therefore, will help increase voter turnout.

The authors of the study describe the implementation and performance of Civitas under various scenarios. This approach allows a realistic but insightful view of the trade-offs of cost, security, and performance.

Foundational Cryptographic Approach: Civitas' design is based on strong cryptographic principles. This ensures that the system is safe. The combination of distributed trust, cryptographic proofs, and secure protocols helps to build strong architecture that protects against many sorts of electoral fraud and safety threats.

Experimental Results: The authors present experimental data that quantify the performance of the system, thus giving a realistic assessment of the scalability and efficiency of Civitas in practice. These results help in understanding the practical consequences of using Civitas in real-world elections.

In general, the strengths of Civitas represent a significant step forward in seeking to find a secure and reliable electronic voting solution that addresses many of the classic problems that electronic voting systems present, all the while opening up new avenues for future research and development in the critical area of democracy.

Weakness(es) of the paper:

While "Civitas: Toward a Secure Voting System" makes a few advances in electronic voting technology, the article has many limitations and faults that should be noted.

Complexity and Usability: The complexity of the Civitas system, along with its heavy reliance on cryptographic protocols and procedures, may present usability problems for ordinary voters. The ability of voters to understand and use any new voting system is an important criterion. Complexity may deter voter participation or introduce errors in the voting process.

Civitas makes specific trust assumptions, such as honesty of the tellers for registration, security of the voter customers, along with some infrastructure, such as secure communication lines and sophisticated cryptographic support, that may not be available or consistently secure in all voting situations.

Scalability Issues: While the paper touches on scalability and offers some experimental results, the real-world scalability of such a system—especially when the same is to be implemented in major national elections that are to cover millions of voters—remains a cause for concern. Computational and logistic difficulties of administering a secure and distributed system of this scale and nature may provide a large set of challenges.

Technical Dependence: The effectiveness of the Civitas lies on the technological competency of the voters and election officials. Ensuring that all players would be comfortable with this level of technological competency is a challenge, especially in less technologically advanced or resource-starved environments.

Cost Issues: Although the paper touches on cost in terms of scalability and performance, the initial setup cost and continuing maintenance costs for such an advanced system may be incompatible for many jurisdictions. This includes the costs of technology, training, and maybe regular updates and security patches.

Field Testing Limitations: The evaluations reported in this paper are experimental and controlled. The system's performance under real-world election conditions, during which a range of unexpected problems related to hardware failures, network malfunctions, and human error may be widespread, has not been tested properly.
Privacy and Security Concerns: No matter how extensive the security features of Civitas, the inherent dangers of digital systems—that is, possible vulnerability to new types of cyber-attacks or breaches of privacy—are not able to be eliminated. The system's reliance on cryptographic techniques could still be vulnerable, one day, to future advances in quantum computing or other technical developments.

These weaknesses do nothing to diminish Civitas' substantial accomplishments but rather point to areas where further research, development, and practical testing is needed to ensure that such a system can be effectively and safely deployed in large numbers.

Reflection

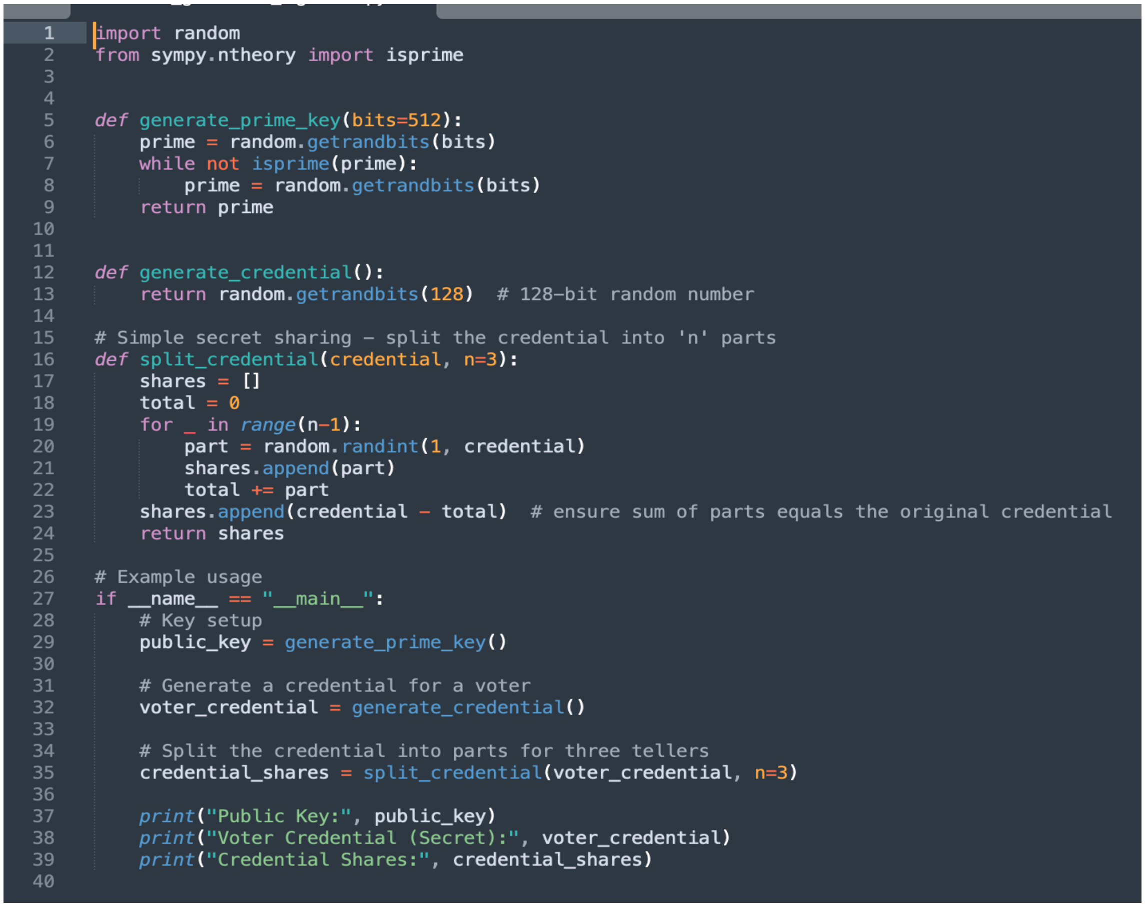
Reading "Civitas: Toward a Secure Voting System," I learned much about the complexity involved in building a secure electronic voting system. It was wonderful as it describes the tradeoffs in balancing security, usability, and cost against each other, highlighting how these factors are varied and difficult to satisfy. The next big areas to improve in this study are to make the system usable to provide accessibility for the most diverse type of voters with various technological skill levels. Further, doing significant real-world testing of the system even during small-scale elections would provide great insight into system performance and user behavior in actual use.

The open and important topic that was not touched upon was how individual device security impacts the integrity of the entire system. This is important because, should there be weaknesses in the voters' devices, it can open the entire system to potential vulnerabilities. The next big thing that could be studied is how to effectively scale Civitas in varying technological infrastructures without compromising security or accessibility. Lastly, the societal, cultural, and political factors that would have a colossal impact on the adoption and success of an advanced electronic voting system such as Civitas.

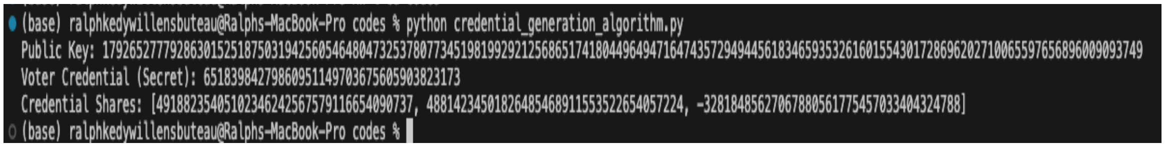
Larger implications of using a system like Civitas exist. This will help to increase democratic participation by making voting more accessible, especially in areas that are not easily accessible. In providing a verifiable and safe voting process, it will increase the level of trust that people place in their election processes, which is essential to democratic institutions' stability and legitimacy. If implemented correctly, it could serve as the beginning for electoral reforms all around the world to provide openness and security in elections.

It raises ethical concerns, especially about the possibility of raising the level of surveillance and abuse. This means that serious management will be needed to ensure that the technology empowers instead of surveilling voters. Establishing proper regulations and standards for electronic voting systems in the process of working with lawmakers will be essential to their integrity and protection of voter data. To summarize, Civitas represents the most significant step in the line of the electronic voting technology that will need to overcome the complex usability, security, and socio-technical challenges.

Extra credit:



```python
import random
from sympy.ntheory import isprime


def generate_prime_key(bits=512):
    prime = random.getrandbits(bits)
    while not isprime(prime):
        prime = random.getrandbits(bits)
    return prime


def generate_credential():
    return random.getrandbits(128)  # 128-bit random number

# Simple secret sharing - split the credential into 'n' parts
def split_credential(credential, n=3):
    shares = []
    total = 0
    for _ in range(n-1):
        part = random.randint(1, credential)
        shares.append(part)
        total += part
    shares.append(credential - total)  # ensure sum of parts equals the original credential
    return shares

# Example usage
if __name__ == "__main__":
    # Key setup
    public_key = generate_prime_key()

    # Generate a credential for a voter
    voter_credential = generate_credential()

    # Split the credential into parts for three tellers
    credential_shares = split_credential(voter_credential, n=3)

    print("Public Key:", public_key)
    print("Voter Credential (Secret):", voter_credential)
    print("Credential Shares:", credential_shares)

```



```
(base) ralphkedywillensbuteau@Ralphs-MacBook-Pro codes % python credential_generation_algorithm.py
 Public Key: 1792652777928630152518750319425605464804732537807734519819929212568651741804496494716474357294944561834659353261601554301728696202710065597656896009093749
 Voter Credential (Secret): 65183984279860951149703675605903823173
 Credential Shares: [49188235405102346242567579116654090737, 48814234501826485468911553522654057224, -32818485627067880561775457033404324788]
(base) ralphkedywillensbuteau@Ralphs-MacBook-Pro codes % 
```