Thesis Project Portfolio

Homomorphic Encryption in Ballot Casting in the Election System

(Technical Report)

The Mutual Influence of Technology, Social Structure, and Public Ideology in Election Systems

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Yufei Zhou

Fall, 2022

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

(Executive summary)

Improving election security and transparency

Democracy's ceremonial, its feast, its great function, is the election.

—H.G. Wells

My STS research paper and technical report are closely related. The election system is the most crucial component of a well-established and authoritative democratic system. In my research paper, I discussed the influence of technology on the U.S. election system throughout history. In the contemporary digitalized world, cyber threats evolved into one of the most adversarial impacts of the election systems. As a result, the public's trust and faith in elections decreased in the past decades due to cybersecurity attacks, misinformation, and the opacity of elections. In my technical report, I proposed a potential solution to resolve the public's concerns regarding the security and transparency of the election system. Specifically, I employed exponential El Gamal encryption and RSA signature schemes.

In my STS research paper, I evaluated the role of technology in different periods of U.S. history. Along with the development of voting techniques, from voice voting to the DREs (Direct Voting Electronics), democratic systems are improved: the elections have become more inclusive and secure. Mainly, I took advantage of Pacey's triangle to fit in cultural, organizational, and technological aspects to discover their mutual influence. It turned out that the advancement in technology both brought advantages and disadvantages to the election system. On the one hand, more rigorous voting technology made the election process more trustworthy. On the other hand, technology came along with different kinds of unprecedented cyber-attacks. After I examined the role of technology in specific times, I analyzed the trend of the evolution of technology's role in society in an overarching perspective with the assistance of technological momentum and technological determinism.

To resolve the concerns in the current election system, I proposed a potential solution—a homomorphic ballot encryption scheme based on the exponential El Gamal algorithm and RSA signature scheme. Homomorphic encryption schemes support mathematical operations on the cipher texts without decryption. This property made a transparent election system possible by posting encrypted ballots online. In contrast to the current election system, voters can trace their votes after cast and make sure their votes will be counted. This electronic voting system will not only rebuild the trust bond between the community and the election system but also improve the accessibility of voting.

These projects are closely related and undoubtedly enriched each other. Together, they produced a systematic procedure:

- A problem was first identified.
- An analysis of the history was then performed.
- A solution was finally proposed.

With technological knowledge, engineers are considered the navigators of the development of society. This research experience further deepened my realization of my responsibility as a computer scientist and my determination to better serve community with my professional skills. My social responsibility motivated me to pursue higher education and to implement my knowledge ethically to produce social values.