Thesis Project Portfolio

Transforming Data Security: Exploring the Potential and Challenges of Homomorphic Encryption in the Digital Age

(Technical Report)

The Encryption Dilemma: Balancing Secure Communication and Lawful Access through Multi-Stakeholder Responsibility

(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

Jonghyun Lee

Spring, 2025

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Introduction

The relationship between my technical capstone project and my STS research paper is rooted in their shared focus on the growing complexities of encryption technologies. My technical project, "Transforming Data Security: Exploring the Potential and Challenges of Homomorphic Encryption in the Digital Age," examines the potential of Homomorphic Encryption (HE) to revolutionize data security by allowing computations on encrypted data without decryption. In parallel, my STS paper, "Encryption, Law Enforcement, and Public Policy: Balancing Privacy and Security in the Digital Age," explores the societal and legal ramifications of widespread encryption technologies, particularly how they complicate criminal investigations. Together, these projects form a comprehensive exploration of both the possibilities and the unintended consequences of encryption in modern society. While they originate from distinct disciplines, working on both projects simultaneously revealed profound intersections between technological advancement and policy challenges, emphasizing the need for a balanced, interdisciplinary approach to digital innovation.

Technical Report

My technical capstone project focuses on the design, implementation, and evaluation of Homomorphic Encryption. HE represents a major breakthrough in cryptographic research by enabling direct computations on encrypted data, preserving confidentiality throughout processing. I implemented HE schemes using Java libraries such as PALISADE and Microsoft SEAL and compared their performance against traditional encryption algorithms like AES and RSA. Through rigorous benchmarking, I evaluated encryption and decryption times, memory

usage, computational overhead, and resilience against known attack vectors, including side-channel attacks. The results highlighted that while HE significantly enhances data privacy, it introduces substantial performance trade-offs: encryption and decryption operations were markedly slower, and memory requirements were significantly higher than those of conventional methods. Nevertheless, HE holds transformative potential, especially for sensitive sectors like healthcare, finance, and national security, where maintaining data confidentiality even during computation is critical. Future work must address the scalability and efficiency challenges to realize HE's widespread adoption.

At the same time, researching the societal impacts of encryption influenced how I approached the technical evaluation of HE. Beyond benchmarking performance metrics, I found myself considering broader ethical questions: How might HE exacerbate the "going dark" problem if widely deployed? Would sectors like law enforcement and cybersecurity require entirely new investigative paradigms to operate in a homomorphically encrypted world? This reflection led me to think critically about the dual-use nature of cryptographic innovations—how technologies designed to enhance privacy could unintentionally empower malicious actors if not paired with thoughtful policy responses. As I designed and tested HE systems, I realized that purely technical excellence was insufficient; responsible innovation demands anticipating how technologies interact with societal infrastructures.

STS Research

Conversely, my STS research paper tackles the societal impacts of encryption advancements. Using Telegram's secret chat feature as a case study, the paper explores how encryption technologies, while protecting users' privacy, have created profound obstacles for law

enforcement agencies worldwide. Telegram's architecture, with device-local secret chats, self-destructing messages, and ephemeral metadata, exemplifies the "going dark" problem—where essential evidence becomes inaccessible due to encryption. Furthermore, the paper examines policy responses like the U.S. CLOUD Act, Australia's TOLA Act, and India's IT Rules, each representing different strategies to reconcile privacy rights with public safety needs. These policies highlight deep tensions between technological progress and regulatory frameworks, often exposing shortcomings in lawmakers' technical understanding. Importantly, the paper emphasizes that although backdoor proposals might seem like straightforward solutions, they introduce systemic security risks that could compromise entire populations' cybersecurity.

Conclusion

Working on these two projects concurrently provided insights that would have been difficult to achieve otherwise. Immersing myself in the technical intricacies of HE made clear why it is practically and ethically difficult to create "responsible encryption" that selectively allows law enforcement access without undermining overall security. The computational and structural realities I encountered while implementing HE paralleled the challenges discussed in my STS research—it became evident that strong encryption inherently resists selective access, not out of corporate stubbornness but because of how securely the systems are mathematically and architecturally constructed. This realization offered a nuanced perspective on policy debates, such as the Apple v. FBI controversy, where technical impossibility, not just political opposition, played a role in resisting government demands.

Ultimately, the experience of working on both projects in tandem reinforced the necessity of holistic thinking in engineering practice. The sociotechnical synthesis between my projects demonstrated that technological innovation cannot be separated from its societal consequences. Engineers developing advanced encryption must remain aware that their work shapes not only data security but also the legal and ethical frameworks that govern modern digital life. Similarly, policymakers crafting legislation around encryption must ground their efforts in technical realities to avoid creating unenforceable or damaging laws. Bridging these worlds is crucial: only through sustained interdisciplinary dialogue can we build a future that upholds both privacy and public safety. The process of pursuing both projects together expanded my technical capabilities while deepening my appreciation of the broader ethical landscape, preparing me to contribute meaningfully to the next generation of secure, responsible technologies.