Algebraic Graph Theory for Cryptographic Protocols

Laasya Vajjala - 11848603
Surya Pramod Vadapalli - 11861342

Overview & Motivation

The evolution of cryptographic protocols has created a pressing need for innovative methods to ensure data integrity and authenticity. Our project explores Algebraic Graph Theory as a foundation for cryptographic protocols, specifically focusing on a novel graph-based digital signature scheme. By leveraging spectral and algebraic properties of graphs (e.g., eigenvalues, spectral gaps), we aim to develop a secure, efficient protocol that ensures message authenticity and integrity.

The motivation stems from the rising interest in post-quantum cryptography, where traditional cryptographic methods may become vulnerable to quantum computing attacks. Graph-based cryptographic schemes offer promising solutions due to their reliance on mathematically complex problems, such as graph isomorphism and eigenvalue computations, which are computationally intensive to reverse-engineer. This project combines mathematical rigor and computational practicality to explore the potential of graph theory in modern cryptographic systems.

Methodology

Our approach involves developing and implementing a digital signature protocol based on the spectral properties of graphs:

1. We will utilize expander graphs (for robustness and efficiency) and Cayley graphs (for their algebraic structure).
2. Keys will be derived from the graph's adjacency matrix and eigenvalues, with private keys involving graph permutations or automorphisms.
3. Messages will be hashed into graph modifications, and their spectral properties (eigenvalues) will form the signature.
4. The protocol will be tested for robustness (spectral gap), resistance to graph isomorphism attacks, and signature uniqueness.

4E Analysis Questions

Our analysis begins with the central question:
"How can spectral and algebraic properties of graphs ensure cryptographic security against tampering, quantum attacks, and uniqueness failures?"

Progress toward generating new questions:
- How does the choice of graph class (expander vs. Cayley) affect performance and security?
- What spectral features contribute most to robustness and resilience against quantum attacks?
- How can graph isomorphism resistance be quantified and enhanced in practical cryptographic implementations?

These questions aim to uncover deeper insights into graph-based cryptographic systems and their potential vulnerabilities.

Expected Individual Contributions

Surya	Mathematical Foundation and Cryptographic Design: - Investigate the algebraic properties of graphs and their cryptographic relevance. - Develop the mathematical framework for key generation and signature schemes. - Focus on spectral analysis and robustness evaluation.
	Report Writing: Theoretical sections
Laasya	Implementation and Testing: - Implement the graph-based cryptographic protocol using Python libraries (e.g., NetworkX, NumPy). - Test and debug the signature generation, verification, and security analysis modules. - Focus on ensuring computational efficiency and practical usability.
	Report writing: Implementation and testing sections
Both	- Both team members will collaborate on generating, analyzing, and interpreting results. - Writing the final report will be a shared effort, ensuring theoretical and practical aspects are cohesively presented.

Conclusion

This project aims to provide a novel perspective on cryptographic protocols by leveraging algebraic graph theory. By combining Laasya's expertise in mathematical analysis and Surya's skills in implementation, we aim to create a robust, post-quantum cryptographic signature scheme. The project also serves as a stepping stone for further exploration into the intersection of graph theory and cryptography.