ABSTRAK

IQBAL FIRMANSYAH. 2025. *Implementasi Teknologi Homomorphic Encryption Untuk Meningkatkan Keamanan Data Pada Aplikasi E-voting Menggunakan Algoritma BFV (Brakersi/Fan-Vercauteren)*, Skripsi. Tanjungpinang: Jurusan Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Univeristas Maritim Raja Ali Haji. Pembimbing I: Hendra Kurniawan, S.Kom., M.Cs.Eng., Ph.D. Pembimbing II: Nurul Hayaty, S.T., M.Cs.

Dalam era kemajuan teknologi informasi, menjaga keamanan dan privasi data menjadi tantangan yang sangat penting, terutama dalam sistem e-voting yang membutuhkan integritas dan kerahasiaan data pemilih. Penelitian ini bertujuan untuk mengimplementasikan teknologi kriptografi homomorfik menggunakan algoritma Brakerski/Fan-Vercauteren (BFV) guna meningkatkan keamanan data dalam aplikasi e-voting. Tidak seperti metode enkripsi konvensional yang hanya mengenkripsi data tanpa memungkinkan pemrosesan lebih lanjut, algoritma BFV memungkinkan pengolahan data langsung dalam bentuk terenkripsi tanpa harus mendekripsinya terlebih dahulu. Metode penelitian meliputi analisis dan penerapan algoritma BFV dalam pembangunan sistem e-voting, proses pembuatan kunci, enkripsi, dan dekripsi data suara. Hasil pengujian menunjukkan bahwa sistem mampu memproses data suara secara aman dalam kondisi terenkripsi, serta lolos dari serangan ciphertext-only attack, di mana data plaintext tidak dapat diungkapkan. Pengujian performa menunjukkan waktu proses enkripsi dan dekripsi rata-rata sebesar 0,012 detik, sementara pengujian Shannon Entropy pada satu data suara terenkripsi menunjukkan nilai sebesar 3,25 bit, yang mencerminkan tingkat kerandoman data yang baik. Dengan demikian, implementasi algoritma BFV pada sistem e-voting memberikan solusi keamanan data yang kuat dan efisien.

Kata kunci: *kriptografi, homomorphic encryption, BFV, enkripsi, dekripsi, e-voting.*

ABSTRACT

IQBAL FIRMANSYAH. 2025. Implementation of Homomorphic Encryption Technology to Enhance Data Security in E-Voting Applications Using the BFV (Brakerski/Fan-Vercauteren) Algorithm. Thesis. Tanjungpinang: Department of Informatics Engineering, Faculty of Engineering and Maritime Technology, Raja Ali Haji Maritime University. Advisor I: Hendra Kurniawan, S.Kom., M.Cs.Eng., Ph.D. Advisor II: Nurul Hayaty, S.T., M.Cs.

In the era of rapid advancement in information technology, ensuring data security and privacy has become a critical challenge, especially in e-voting systems that require the integrity and confidentiality of voter data. This study aims to implement homomorphic cryptography technology using the Brakerski/Fan-Vercauteren (BFV) algorithm to enhance data security in e-voting applications. Unlike conventional encryption methods that merely encrypt data without allowing further processing, the BFV algorithm enables data to be processed directly in its encrypted form without the need for decryption. The research method involves analyzing and applying the BFV algorithm in the development of an e-voting system, including the key generation process, as well as data encryption and decryption. The results indicate that the system can securely process voting data while still encrypted and withstand ciphertext-only attacks, where plaintext data cannot be revealed. Performance testing shows an average encryption and decryption time of 0.012 seconds, while the Shannon Entropy test on a single encrypted vote yields a value of 3.25 bits, reflecting a high level of data randomness. Therefore, the implementation of the BFV algorithm in the e-voting system provides a strong and efficient data security solution.

Keywords: *cryptography, homomorphic encryption, BFV, encryption, decryption, e-voting.*