# BAB I
# PENDAHULUAN

## A. Latar Belakang

Di era digital yang semakin maju, kebutuhan akan sistem keamanan data yang kuat dan efisien semakin mendesak, terutama dalam menjaga kerahasiaan informasi sensitif seperti data pribadi, transaksi keuangan, serta sistem kritis seperti e-voting. Dalam konteks keamanan data, penerapan algoritma enkripsi yang mampu memberikan perlindungan kuat tanpa mengorbankan efisiensi komputasi menjadi fokus utama.

Algoritma BFV (Brakerski/Fan-Vercauteren) sangat penting dalam perhitungan suara pada aplikasi *e-voting* karena memberikan solusi yang menggabungkan keamanan dan efisiensi yang diperlukan dalam pemilu elektronik. Dalam *e-voting*, data suara merupakan informasi yang sangat sensitif, sehingga diperlukan perlindungan tingkat tinggi untuk menjaga kerahasiaan pilihan pemilih. BFV memungkinkan perhitungan dilakukan langsung pada data terenkripsi tanpa perlu mendekripsi terlebih dahulu, menjaga privasi suara sepanjang proses perhitungan dan mengurangi risiko manipulasi oleh pihak yang tidak berwenang. Selain itu, kemampuan BFV untuk melakukan operasi matematika secara langsung pada *ciphertext* membuat proses perhitungan menjadi lebih efisien dan akurat, tanpa mengorbankan keamanan data [1].

Algoritma ini juga kompatibel dengan infrastruktur modern, seperti sistem *cloud*, yang sering digunakan dalam aplikasi *e-voting*. Hal ini memudahkan integrasi BFV ke dalam sistem yang ada, memastikan perhitungan dapat dilakukan dengan cepat dan aman. Selain itu, BFV dirancang untuk tahan terhadap berbagai jenis serangan kriptografi, termasuk serangan berbasis quantum, sehingga mampu melindungi integritas data suara dari ancaman yang dapat menggagalkan proses pemilu. Dengan kelebihan ini, penggunaan algoritma BFV dalam *e-voting* tidak hanya menjawab kebutuhan akan keamanan dan privasi, tetapi juga memastikan bahwa perhitungan suara dapat dilakukan dengan efisien dan dapat diandalkan [2].

## B. Perumusan Masalah

Bagaimana efektifitas algoritma BFV dalam mengamankan data pada aplikasi *e-voting* ?

## C. Batasan Penelitian

Penelitian ini akan difokuskan pada penerapan algoritma BFV dalam konteks enkripsi homomorfik untuk sistem keamanan data pada aplikasi *e-voting*. Studi ini terbatas pada skenario *e-voting*, tanpa mempertimbangkan penerapan BFV di bidang lain. Analisis akan terbatas pada aspek teknis dan kinerja algoritma BFV, tanpa membahas aspek hukum, etika, atau regulasi terkait enkripsi dalam *e-voting*. Penelitian ini juga tidak akan mendalami teknik *"bootstrapping"* untuk konversi dari *somewhat homomorphic encryption (SHE) ke fully homomorphic encryption (FHE)*.

## D. Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisis penerapan algoritma BFV *(Brakerski/Fan-Vercauteren)* dalam meningkatkan keamanan data pada aplikasi e-voting, serta mengevaluasi kinerja dan efisiensinya dalam pengolahan data terenkripsi. Penelitian ini juga bertujuan untuk mengidentifikasi tantangan dan potensi yang muncul dalam penggunaan algoritma BFV pada skenario e-voting, serta membandingkan tingkat keamanannya dengan metode enkripsi lain. Selain itu, penelitian ini akan memberikan rekomendasi untuk optimalisasi penerapan algoritma BFV guna memastikan keamanan dan integritas data suara.

## E. Manfaat Penelitian

1. Membantu pengembangan sistem e-voting yang lebih aman dengan penerapan algoritma BFV, sehingga meningkatkan perlindungan data pemilih dan integritas hasil pemungutan suara.
2. Memberikan kontribusi pada optimalisasi enkripsi homomorphic dengan meningkatkan efisiensi dan performa enkripsi dalam aplikasi dunia nyata.

3. Menambah literatur dan wawasan di bidang kriptografi, khususnya terkait penerapan dan tantangan algoritma BFV dalam konteks keamanan data.
4. Menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan keamanan data dan penerapan enkripsi di berbagai sektor.