INTISARI

Algoritma Dekoding pada Kode Reed-Muller Termodifikasi

Oleh

Purnama Sari

22/495513/PPA/06307

Teori pengkodean mempelajari cara-cara untuk mengkodekan informasi dengan tujuan meningkatkan efisiensi dan keamanan dalam transmisi data. Salah satu aplikasi teori pengkodean adalah aplikasi pada kriptografi, seperti sistem kriptografi McEliece yang menggunakan kode Goppa. Namun, sistem ini memerlukan parameter yang besar dan proses verifikasi yang lambat. Pada tahun 2017, Lee dkk. mengembangkan skema tanda tangan digital pqsigRM dengan mengganti kode Goppa menggunakan kode Reed-Muller tertusuk, yang lebih cepat dan lebih efektif. Pada tahun 2020, skema sebelumnya dimodifikasi menjadi skema modified pqsigRM yang lebih aman dan efisien. Penelitian ini bertujuan untuk mengkaji modifikasi kode Reed-Muller dan algoritma dekodingnya untuk meningkatkan efisiensi dan keamanan skema tanda tangan digital. Penelitian juga disertai implementasi program C untuk komputasi kode Reed-Muller termodifikasi dan dekodingnya, yang diharapkan dapat menghasilkan tanda tangan digital dengan ukuran kunci yang lebih kecil dan proses verifikasi yang lebih cepat.

ABSTRACT

Decoding Algorithm of Modified Reed-Muller Codes

By

Purnama Sari

22/495513/PPA/06307

Coding theory studies ways to encode information in order to improve efficiency and security in data transmission. One application of coding theory is the application in cryptography, such as the McEliece cryptography system that uses the Goppa code. However, this system requires large parameters and a slow verification process. In 2017, Lee et al. developed a pqsigRM digital signature scheme by replacing the Goppa code with a punctured Reed-Muller code, which is faster and more effective. In 2020, the previous scheme was modified into a modified pqsigRM scheme that is more secure and efficient. This study aims to examine the modification of the Reed-Muller code and its decoding algorithm to improve the efficiency and security of the digital signature scheme. The study is also accompanied by the implementation of a C program for computing the modified Reed-Muller code and its decoding, which is expected to produce a digital signature with a smaller key size and a faster verification process.