Jurnal Riset Mahasiswa Matematika
Volume 4(3) (2025), Pages 128-132
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Implementasi Kode Goppa dalam Kriptosistem McEliece untuk Keamanan Data Terhadap Serangan Kuantum

Lili Khoiriyah, Muhammad Khudzaifah*, Erna Herawati

Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

Email: khudzaifah@uin-malang.ac.id

Abstrak

Keamanan data dalam era digital semakin penting, khususnya dalam menghadapi ancaman komputasi kuantum terhadap algoritma kriptografi klasik. Salah satu kandidat utama kriptografi pasca-kuantum adalah kriptosistem McEliece, yang menggunakan kode koreksi kesalahan untuk memperkuat proses enkripsi. Penelitian ini mengimplementasikan kode Goppa dalam kriptosistem McEliece untuk meningkatkan ketahanan terhadap serangan kuantum. Pada penelitian ini digunakan polinomial berderajat dua pada lapangan hingga dengan 16 elemen, menghasilkan parameter kode dengan panjang dua belas, dimensi empat, dan kapasitas koreksi dua kesalahan. Proses enkripsi dilakukan dengan mengalikan pesan dalam bentuk biner dengan kunci publik serta menambahkan vektor kesalahan acak, sedangkan dekripsi menggunakan kunci privat untuk memperbaiki kesalahan melalui perhitungan sindrom. Hasil penelitian menunjukkan bahwa penggunaan kode Goppa meningkatkan keamanan sistem dengan memperumit struktur ciphertext, sehingga memperkuat ketahanan terhadap serangan berbasis kuantum. Implementasi ini membuktikan bahwa teknik pengkodean klasik tetap relevan dan efektif dalam mendukung kriptografi modern.

Kata kunci: Kode Goppa; Kriptosistem McEliece; Kriptografi Pasca-Kuantum; Keamanan Data; Kode Koreksi Kesalahan

Abstract

The importance of data security in the digital era is growing, particularly in the face of quantum computing threats against classical cryptographic algorithms. One of the main candidates for post-quantum cryptography is the McEliece cryptosystem, which employs error-correcting codes to enhance encryption strength. This study implements Goppa codes within the McEliece cryptosystem to increase resistance against quantum attacks. A degree-two polynomial over a finite field with sixteen elements was used, resulting in code parameters with a length of twelve, a dimension of four, and the ability to correct two errors. Encryption is carried out by multiplying the binary message with the public key and adding a random error vector, while decryption utilizes the private key to correct errors through syndrome calculation. The results demonstrate that employing Goppa codes enhances system security by complicating the ciphertext structure, thereby strengthening resilience against quantum-based attacks. This implementation confirms that classical coding techniques remain relevant and effective in supporting modern cryptography.

Keywords: Goppa Code; McEliece Cryptosystem; Post-Quantum Cryptography; Data Security; Error-Correcting.

Submitted: 27 Desember 2024 Reviewed: 13 Februari 2024 Accepted: 24 Februari 2025
Doi: http://dx.doi.org/10.18860/jrmm.v4i3.31212

PENDAHULUAN

Di era digital saat ini, keamanan dalam pengiriman pesan menjadi isu yang sangat penting. Banyaknya penyalahgunaan selama proses pengiriman pesan melalui jaringan internet menuntut peningkatan perlindungan terhadap kerahasiaan informasi. Sistem digital dianggap sebagai pilihan terbaik untuk pengiriman pesan jarak jauh, namun ketika data harus ditransmisikan dalam jarak ratusan hingga ribuan kilometer, risiko terjadinya kesalahan transmisi meningkat [1]. Kesalahan ini dapat disebabkan oleh gangguan pada saluran atau interferensi eksternal yang menyebabkan perbedaan antara pesan yang dikirim dan pesan yang diterima.

Masalah dalam transmisi data tidak berhenti pada kesalahan teknis saja. Dengan perkembangan teori pengkodean, muncul tantangan baru terkait keamanan dalam pengiriman pesan melalui komputer atau jaringan internet. Internet sebagai media publik memungkinkan akses bebas, sehingga meningkatkan risiko penyadapan oleh pihak tidak berwenang [2]. Kondisi ini mendorong kebutuhan mendesak akan mekanisme perlindungan data atau informasi untuk menjaga privasi pengguna. Salah satu bidang ilmu yang berfokus pada perlindungan informasi ini adalah kriptografi, yang mempelajari metode-metode pengamanan pesan melalui penyandian [3][4][5].

Dalam kriptografi, digunakan teknik matematika untuk mengubah data asli menjadi bentuk terenkripsi sehingga hanya dapat dipahami oleh pihak yang berwenang [6]. Salah satu pendekatan utama adalah penggunaan algoritma kunci publik atau algoritma kunci asimetris [7]. Pada sistem ini, kunci publik digunakan untuk proses enkripsi, sedangkan kunci privat digunakan untuk dekripsi [8]. Meskipun efektif, algoritma kunci publik konvensional dinilai rentan terhadap serangan berbasis komputasi kuantum, sehingga perlunya sistem kriptografi yang lebih kuat menjadi perhatian utama.

Kriptosistem McEliece merupakan salah satu kandidat kuat untuk standarisasi kriptografi pasca-kuantum. Sistem ini memanfaatkan sifat acak dalam proses enkripsinya sehingga lebih tahan terhadap serangan berbasis algoritma kuantum [9][10]. Dalam implementasinya, McEliece menggunakan kode linier tersembunyi berbasis error-correcting code untuk menjaga keamanan pesan. Beberapa penelitian mengembangkan varian McEliece menggunakan kode Generalized Reed Solomon untuk memperkecil ukuran kunci dan mempercepat implementasi perangkat lunak maupun perangkat keras [11]. Namun demikian, tantangan utama tetap terletak pada optimalisasi efisiensi dan penguatan keamanan sistem terhadap serangan struktural.

Kode error-correcting, khususnya kode Goppa, telah diakui memiliki keunggulan dalam memperkuat kriptosistem McEliece. Kode Goppa menawarkan kapasitas koreksi kesalahan yang tinggi dan menghasilkan struktur matriks parity-check yang sulit dibedakan dari matriks acak, menjadikannya lebih resisten terhadap serangan struktural [12][13][14]. Selain itu, pertumbuhan eksponensial jumlah kode yang tidak ekuivalen berdasarkan parameter kode membuat analisis serangan menjadi lebih kompleks [15].

Penelitian ini berkontribusi dengan mengimplementasikan kode Goppa menggunakan polinomial sederhana dalam lapangan hingga kecil, serta menerapkan simulasi enkripsi dan dekripsi terhadap pesan berbasis ASCII. Kebaruan yang ditawarkan terletak pada analisis implementasi kode Goppa dengan parameter kode kecil, yang menunjukkan efektivitasnya dalam memperkuat kriptosistem McEliece terhadap potensi serangan kuantum. Dengan pendekatan ini, penelitian ini mempertegas relevansi teknik pengkodean klasik dalam menghadapi tantangan keamanan modern.

METODE PENELITIAN

Jenis Penelitian

Penelitian ini termasuk jenis penelitian kualitatif, dimana penelitian diambil dari sebuah data yang kemudian memanfaatkan teori yang ada sebagai bahan untuk penjelas. Metode penelitian yang digunakan adalah studi literatur yang bertujuan untuk mengembangkan aspek teoritis. Metode ini sangat berguna untuk mengidentifikasi pengetahuan yang belum diketahui, mengembangkan teori baru, atau merancang kerangka dasar untuk penelitian lebih lanjut dalam

berbagai bidang ilmu pengetahuan. Dengan demikian, penelitian ini memungkinkan peneliti untuk memahami suatu masalah atau fenomena hanya dengan menganalisis dari buku atau jurnal.

Tahapan Penelitian

1. Proses dan simulasi pembangkitan kunci untuk implementasi kode Goppa dalam kriptosistem McEliece.
   a. Pilih polinomial $g(x) = x^2 + a^7x + 1$ dengan derajat t atas $GF(2^4)$ dengan parameter kode dengan panjang $n = 12$, dimensi $k = 4$, dan koreksi kesalahan $t = 2$.
   b. Menentukan matriks generator berukuran 4×12 yang dibangkitkan berdasarkan parameter kode Goppa.
   c. Menentukan matriks permutasi P berukuran 12×12, di mana P adalah matriks yang memuat 1 pada setiap baris dan setiap kolom.
   d. Menentukan secara acak matriks S berukuran 4×4 yang merupakan matriks non-singular.
   e. Kemudian menghitung G' dengan ukuran 4×12 dengan perkalian ketiga matriks yaitu $G' = SGP$.
2. Proses enkripsi dan simulasi pesan pada kriptosistem McEliece menggunakan kode Goppa.
   a. Menentukan pesan sebagai plaintext, kemudian mengubah ke bentuk binary berdasarkan tabel ASCII sebagai binary string m dengan panjang k. Pada penelitian ini, saya menggunakan pesan "KAMU".
   b. Pesan m dikalikan dengan kunci publik G'.
   c. Menentukan vektor *error* e (vektor dengan panjang n dan bobot t).
   d. Menambahkan kesalahan pada codeword $C_i' = mG' + e$.
3. Proses deskripsi dan simulasi pesan pada kriptosistem McEliece menggunakan kode Goppa.
   a. Menghitung invers dari matriks P.
   b. Menghitung $Y_i = C_i' \times P^{-1}$.
   c. Menggunakan algoritma decoding sehingga diperoleh $\hat{m}$.
   d. Menghitung $m = \hat{m}S^{-1}$.

HASIL DAN PEMBAHASAN

Proses Pembangkitan Kunci

Proses pembentukan kunci dalam kriptosistem McEliece memiliki peran krusial dalam memastikan keamanan dan efisiensi sistem. Pada tahap ini, dua jenis kunci yang dibangkitkan yaitu kunci privat dan kunci publik. Proses ini dilakukan oleh pihak penerima, sehingga hanya penerima yang memiliki akses terhadap kunci privat yang digunakan. Tahapan ini dimulai dengan menentukan nilai n dan k, yang digunakan untuk membangun matriks generator G. Pada penelitian ini ditentukan parameter kode berdasarkan kode Goppa $\Gamma(L, g(x))$, dimana $g(x) = x^2 + a^7x + 1$ dan $L = \{\alpha^i | 2 \leq i \leq 13\}$, Sehingga diperoleh $n = 12$ dan $k = 4$.

Tahap berikutnya adalah membentuk kunci privat G berupa matriks generator berukuran $k \times n$ berdasarkan parameter kode Goppa $\Gamma(L, g(x))$. Selanjutnya kunci privat S, yaitu matriks non-singular berukuran $k \times k$, dibuat dengan memilih sembarang matriks berukuran $k \times k$ dan memeriksa determinannya untuk memastikan sifat non-singular. Untuk kunci privat P, matriks permutasi berukuran $n \times n$ dipilih secara acak. Tahapan terakhir yaitu pembangkitan kunci publik G' dengan menghitung $G' = SGP$ yang akan menghasilkan matriks berukuran $k \times n$.

Proses Enkripsi

Proses enkripsi dalam kriptosistem McEliece memanfaatkan kode koreksi error untuk melindungi informasi rahasia. Proses enkripsi dilakukan oleh pengirim, adapun tahap enkripsi diawali dengan memilih pesan plaintext yang akan di enkripsi, kemudian pesan tersebut dikonversi menjadi vektor biner berdasarkan tabel ASCII 256-bit sehingga diperoleh pesan m

berupa vektor biner. Kemudian vektor kode biner pesan m dibagi menjadi blok-blok vektor dengan panjang yang sesuai dengan dimensi kode, yaitu k. Selanjutnya membuat vektor kesalahan e dengan panjang n yang memiliki bobot maksimum kesalahan t. Vektor biner pesan m selanjutnya dikalikan dengan kunci publik G'. Hasil perkalian tersebut berupa vektor ciphertext yang kemudian ditambahkan dengan vektor error acak e seperti rumus berikut $C_i' = mG' + e$. Penambahan vektor *error* ini meningkatkan kompleksitas, sehingga menyulitkan pihak yang tidak berwenang untuk melakukan dekripsi.

Proses Dekripsi

Proses dekripsi dalam kriptosistem McEliece adalah langkah untuk mengubah ciphertext yang diterima kembali menjadi pesan plaintext asli. Proses ini hanya dapat dilakukan oleh penerima yang memiliki kunci privat, yang terdiri dari matriks $\boldsymbol{P}$, $\boldsymbol{S}$ dan $\boldsymbol{G}$. Dekripsi bertujuan untuk menghilangkan efek permutasi dan *error* yang ditambahkan selama enkripsi, sehingga pesan asli dapat direkontruksi secara akurat.

Proses ini dimulai dengan menerima ciphertext yang telah dienkripsi dengan menggunakan kunci publik $\boldsymbol{G}'$. Kemudian mengalikan dengan invers dari matriks permutasi $\boldsymbol{P}$ untuk menghapus permutasi yang telah diterapkan pada proses enkripsi yang menghasilkan vektor $\boldsymbol{y}$. Selanjutnya, dihitung syndrome $\boldsymbol{s}(\boldsymbol{x})$ menggunakan $\boldsymbol{s}(\boldsymbol{x}) \equiv \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \frac{\boldsymbol{y_i}}{\boldsymbol{x-\alpha_i}}$, yang digunakan untuk mendeteksi *error*. Lokasi error ditentukan melalui polinomial error *locator* $\boldsymbol{\sigma}(\boldsymbol{x})$, dan bit-bit yang salah diperbaiki berdasarkan lokasi error tersebut, sehingga diperoleh vektor kode $\widehat{\boldsymbol{m}}$. Setelah error diperbaiki, efek matriks transformasi dihilangkan dengan mengalikan $\widehat{\boldsymbol{m}}$ dengan invers matriks $\boldsymbol{S}$, menghasilkan vektor pesan asli $\boldsymbol{m}$. Terakhir, vektor biner $\boldsymbol{m}$ dikonversi kembali ke bentuk teks menggunakan tabel ASCII, sehingga pesan plaintext yang sesuai dengan pesan awal dapat diperoleh.

KESIMPULAN

Berdasarkan dari pembahasan di atas didapatkan kesimpulan bahwa implementasi kode Goppa pada kriptosistem McEliece dengan menggunakan polinomial $g(x) = x^2 + \alpha^7 x + 1$ pada $GF(2^4)$ didapatkan parameter kode Goppa dengan panjang $n = 12$ dan dimensi kode $k = 4$ dengan tingkat kesalahan $t = 2$ menunjukkan teknik pengkodean klasik dapat digunakan untuk proses enkripsi pada kriptografi modern. Penambahan error e pada pesan m_i yang telah dikalikan dengan kunci publik G', menciptakan ciphertext yang menyulitkan untuk dekripsi tanpa kunci privat. Penambahan error acak ini memberikan keamanan tambahan, yang menjadikan proses enkripsi sebagai langkah penting dalam menjaga kerahasiaan dan keamanan pesan.

Selanjutnya, kode Goppa digunakan untuk menghitung syndrome $s(x)$, yang mendeteksi error dan menentukan lokasi bit yang salah. Proses koreksi error ini memungkinkan penerima untuk memulihkan pesan asli. Sehingga, dengan memanfaatkan polinomial untuk menentukan parameter kode memberikan kemampuan koreksi error yang tinggi, sehingga membuat sistem lebih sulit untuk dipecahkan oleh algoritma serangan yang berbasis kuantum. Dengan mengimplementasikan kode Goppa dalam kriptosistem McEliece menunjukkan bahwa sistem ini dapat meningkatkan keamanan pertukaran informasi dan menangani ancaman dari komputer kuantum.

DAFTAR PUSTAKA

[1] Anggraeni, W. (2004). Deteksi Dan Koreksi Kesalahan Informasi Dalam Sandi Biner Dengan Menggunakan Metode Hamming. JUTI, 3, 101-108.

[2] Ariyus , D. (2008). *Pengantar Ilmu Kriptografi.* Yogyakarta: ANDI.

[3] Ziaurrahman, M., Utami, E., & Wibowo, F. W. (2019). Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut. *Jurnal Informasi Interaktif, Vol.4*.

[4] Prayitno, A., & Nurdin. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition. *JESIK:Jurnal Elektronik Sistem Informasi dan Komputer, 3*.

[5] Waliprana, W. E. (2011). *Studi dan Implementasi Algoritma kunci publik McEliece.* Bandung: Makalah, Institut Teknologi Bandung.

[6] Siim, S. (2015). Study of McEliece Cryptosystem. *Research Seminar in Seminar Crytography*.

[7] Surnawani, Jarkasih, S., & Fatimah, U. (2022). Penggunaan Public Key Infrastructure Kunci Persetujuan (Key Agreement). *TripleA : Jurnal Pendidikan Teknologi Informasi* , 97-102.

[8] Niven, I., Zuckerman, H. S., & Montgomery, H. L. (1980). *An Introduction to the Theory of Numbers* (Fifth edition ed.). New York: John Wiley and Sons, 1991.

[9] Ling, S., & Xing, C. (2004). *Coding Theory.* New York: Cambridge University Press.

[10] Sadikin , R. (2012). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: C.V. ANDI OFFSET.

[11] Childs, L. N. (2019). *Cryptology and Error Correction.* New York: Springer International Publishing.

[12] Stallings, W. (2003). *Cryptography and Network Security.* New Jersey: Pearson Education.

[13] Singh, H. (2020). *Code based Cryptography: Classic McEliece.*

[14] Rosdiana. (2015). Sekuritas Sistem Dengan Kriptografi. *al-Khwarizmi*, 21-32.

[15] Chen, B., & Zhang, G. (2023). *The number of extended irreducible binary Goppa codes.* China: IEEE Transactions on Information Theory.