Prosiding Seminar Nasional Matematika dan Pendidikan Matematika (SESIOMADIKA) 2025
Tema: Mendidik dengan matematika, membentuk dunia dengan data: Peran pendidikan matematika, pemodelan dan machine learning dalam era peradaban cerdas

Penerapan Kode Bose Chaudhuri Hocquenghem pada Kriptosistem Niederreiter

Chika Bunga Permata*
Universitas Sebelas Maret, *Penulis Korespondensi: chikabunga2284@student.uns.ac.id

Putranto Hadi Utomo
Universitas Sebelas Maret

Tri Atmojo Kusmayadi
Universitas Sebelas Maret

ABSTRAK

Penelitian ini bertujuan untuk menerapkan dan menganalisis penggunaan Kode BCH (Bose Chaudhuri Hocquenghem) pada Kriptosistem Niederreiter sebagai upaya meningkatkan keamanan data terhadap ancaman komputasi kuantum. Metode yang digunakan berupa kajian pustaka dengan mengacu pada berbagai sumber seperti buku, jurnal, dan skripsi yang membahas kode BCH dan Kriptosistem Niederreiter. Proses penelitian meliputi tiga tahap utama, yaitu pembangkitan kunci, enkripsi, dan dekripsi. Pada tahap pembangkitan kunci dibentuk matriks paritas BCH H, matriks acak invertibel S, serta matriks permutasi P, yang kemudian dikombinasikan menjadi kunci publik $H' = S \cdot H \cdot P$. Proses enkripsi dilakukan dengan membentuk vektor kesalahan e dan menyembunyikan pesan serta menghasilkan *ciphertext* berupa sindrom $c = H' \cdot e^T$. Pada tahap dekripsi, diperoleh sindrom internal $c' = S^{-1} \cdot c$, kemudian dilakukan *decoding* BCH untuk menemukan posisi kesalahan dan mengembalikan vektor asli $e = P^{-1} \cdot e'$. Hasil penelitian menunjukkan bahwa vektor kesalahan e yang diperoleh pada tahap akhir sama dengan vektor kesalahan asli yang digunakan saat enkripsi. Vektor e merupakan hasil dekripsi dari pesan rahasia yang sesuai dengan *ciphertext* c. Sehingga, kombinasi Kode BCH dengan Kriptosistem Niederreiter menghasilkan sistem enkripsi yang efisien, aman, dan mampu mengoreksi kesalahan dengan tepat.

Kata kunci: Dekripsi, enkripsi, kode bch, kriptografi, kriptosistem niederriter

PENDAHULUAN

Di era serba digital dan serba cepat, komunikasi berfungsi sebagai elemen krusial dalam kehidupan sehari-hari. Inovasi dalam teknologi internet memudahkan interaksi dan pertukaran data serta informasi melalui jaringan digital. Meski begitu, jaringan digital juga menghadapi risiko terkait masalah keamanan informasi, seperti penyadapan dan kebocoran data penting. Dengan demikian, perlindungan terhadap kerahasiaan dan keamanan data menjadi kebutuhan mendesak.

Kriptografi merupakan metode untuk menjaga informasi dari akses yang tidak sah. Secara umum, kriptografi memungkinkan pengirim pesan untuk mengubah pesan asli (*plaintext*) menjadi pesan yang telah terenkripsi (*ciphertext*) melalui proses enkripsi. Penerima pesan dapat memulihkan pesan asli melalui proses dekripsi dengan menggunakan informasi rahasia berupa kunci privat. Dengan demikian, meskipun pihak ketiga berhasil mendapatkan *ciphertext* tetap tidak dapat memulihkan pesan asli tanpa kunci privat yang valid (Utami, 2011).

Selama beberapa dekade terakhir, metode kriptografi klasik seperti RSA (*Rivest Shamir Adleman*) dan ECC (*Elliptic Curve Cryptography*) menjadi standar keamanan yang luas digunakan. Namun, kemajuan perkembangan komputasi kuantum menghadirkan ancaman serius terhadap keamanan sistem tersebut. Algoritma kuantum memiliki kemampuan menyelesaikan permasalahan matematika kompleks yang mendasari keamanan RSA dan ECC dalam jangka waktu jauh lebih singkat dibandingkan dengan komputer klasik

(Bernstein *et al*., 2009). Kondisi ini menekankan pentingnya pengembangan sistem kriptografi yang tahan terhadap serangan kuantum.

Sebagai salah satu alternatif, Kriptosistem Niederreiter diperkenalkan oleh Harald Niederreiter pada tahun 1986 sebagai modifikasi dari Kriptosistem McEliece. Sistem ini memanfaatkan matriks paritas dari kode koreksi kesalahan sebagai kunci publik, sehingga proses enkripsi dan dekripsi menjadi lebih efisien (Niederreiter, 1986). Keunggulan lainnya adalah keamanan sistem ini bergantung pada masalah *decoding* kode yang secara matematis terbukti sulit untuk dipecahkan, sehingga relatif aman terhadap serangan kuantum yang ada saat ini. Pada penelitian sebelumnya, Kriptosistem Niederreiter memanfaatkan Kode Goppa dalam tahapan enkripsi dan dekripsi. Namun, seiring berjalannya waktu berbagai kode koreksi kesalahan lainnya telah dikembangkan, salah satunya adalah Kode BCH (*Bose Chaudhuri Hocquenghem*). Kode BCH adalah perluasan dari Kode Hamming, dirancang untuk koreksi kesalahan berganda dan telah banyak diterapkan dalam sistem komunikasi digital.

Pemilihan Kode BCH dalam Kriptosistem Niederreiter juga dipengaruhi oleh keterbatasan dari penelitian sebelumnya, yang umumnya hanya meneliti kombinasi Kode BCH dengan Kriptosistem McEliece atau penggunaan kode lain (seperti Kode Goppa dan Kode Hamming) pada Niederreiter. Oleh karena itu, tujuan dari penelitian ini adalah untuk menerapkan dan mengimplementasikan Kriptosistem Niederreiter berbasis Kode BCH, sebagai upaya untuk mengembangan sistem keamanan informasi yang tahan terhadap ancaman komputasi kuantum.

METODE

Metode penelitian yang digunakan dalam penelitian ini yaitu kajian pustaka dengan menggunakan beberapa referensi berupa buku, tesis, artikel, jurnal serta skripsi mengenai Kode BCH, Kriptosistem Niederreiter. Terdapat 3 langkah yang dilakukan dalam penelitian ini, yaitu pembangkitan kunci, proses enkripsi pesan, dan proses dekripsi.

Pembangkitan Kunci

Langkah-langkah dalam pembangkitan kunci sebagai berikut.

Memilih kode linier BCH $[n, k]$ yang dapat memperbaiki t eror dengan panjang kode $n = 2^m - 1$.

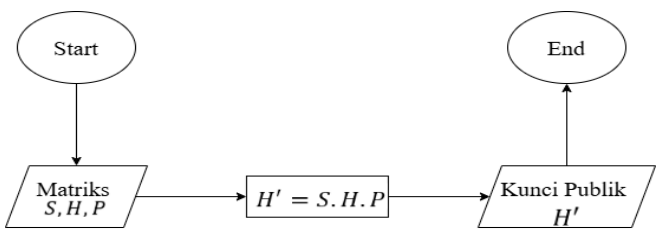
Membangun matrik paritas H dengan menetukan polinomial generator $g(x)$ dari Kode BCH sehingga dibentuk matrik paritas H berukuran $(n-k) \times n$.

Membangkitkan matriks *invertible* acak S. Pengirim membangkitkan matrik *invertible* S berukuran $(n-k) \times (n-k)$. Matriks ini berfungsi untuk menyamarkan struktur asli Kode BCH.

Membangkitkan matriks permutasi P berukuran $(n \times n)$. Matriks ini diperoleh dari matriks identitas yang dilakukan pengacakan pada kolomnya.

Menghitung kunci publik dengan persamaan $H' = S \cdot H \cdot P$, dimana H'merupakan matriks paritas hasil transformasi yang akan digunakan untuk proses enkripsi pesan.

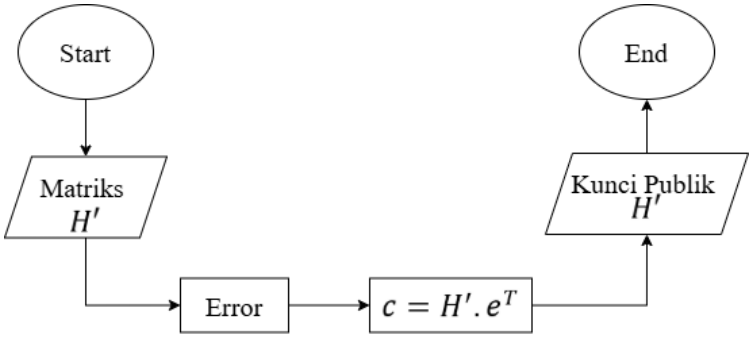
Kunci privat terdiri dari (S, H, P) yang disimpan secara rahasia oleh pengirim.



Gambar 1. Flowchart Pembangkitan Kunci

Proses Enkripsi Pesan

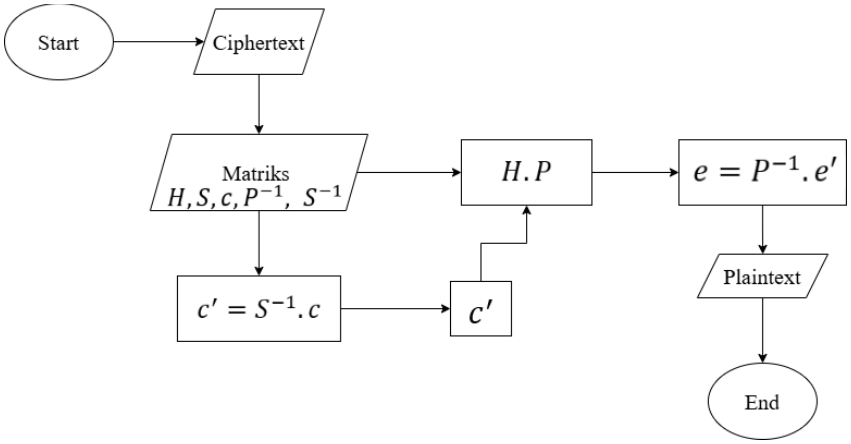
1. Pembentukan vektor eror. Pengirim membangkitkan vektor eror acak e sepanjang n dengan bobot Hamming t sebagai *plaintext.*
2. Perhitungan sindrom dengan menggunakan kunci publik H' untuk menghitung *ciphertext* c berupa sindrom $c = H' \cdot e^T$.
3. Pengiriman *ciphertext* c dikirimkan ke penerima. Karena c hanya berupa sindrom hasil perkalian linier, pesan yang dikirimkan sangat ringkas (tidak langsung mengandung striktur e).



Gambar 2. Flowchart Proses Enkripsi

Proses Dekripsi Pesan

1. Penerima menerima *ciphertext* berupa c (sindrom) $c = H'.e^T$
2. Menghitung sindrom terhadap Kode BCH asli dengan persamaan $c' = S^{-1} \cdot c$.
3. Penerima melakukan *decode* sindrom dengan Kode BCH. *Decode* dilakukan dengan mencocokan sindrom c terhadap matriks $H \cdot P$ untuk menemukan posisi bit eror.
4. Penerima melakukan pembatalan permutasi pada kolom P untuk memperoleh vektor eror asli $e = P^{-1} \cdot e'$.
5. Vektor eror e merupakan hasil dekripsi dan pesan rahasia yang sesuai dengan *ciphertext* c.



Gambar 3. Flowchart Proses Dekripsi

HASIL DAN PEMBAHASAN

Pada bab ini diberikan hasil dan pembahasan penerapan Kode BCH pada Kriptosistem Niederreiter.

Pembangkitan Kunci

Pada proses pembangkitan kunci, pengguna menggunakan metode Kode BCH untuk menentukan parameter kunci (n) dan (k), yang pada contoh ini diberikan nilai $(n = 7)$ dan $(k = 4)$. Selanjutnya, matriks paritas *check* (H) ditentukan sebagai berikut.

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Setelah itu, dilakukan pembangkitaan matriks (S) secara acak dengan dimensi $(n-k) \times (n-k)$ dan matriks (P) dengan dimensi $(n \times n)$.

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Kemudian dilakukan perkalian matriks S, H, P untuk memperoleh nilai matriks H'.

$$H' = S \cdot H \cdot P$$

$$H' = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Dengan demikian, diperoleh matriks

$$H' = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Proses Enkripsi Pesan

Pada tahap enkripsi, proses dilakukan berdasarkan prinsip dasar Kriptosistem Niederreiter, yaitu pembentukan *ciphertext* dalam bentuk sindrom. Pengirim membentuk vektor kesalahan (*eror vector*) yang akan digunakan untuk menghasilkan *ciphertext.* Vektor ini memiliki panjang 7-bit dan bobot Hamming $t = 1$, yang berarti hanya satu bit bernilai 1. Selanjutnya vektor eror ditentukan sebagai berikut.

$$e = [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]$$

Menghitung sindrom untuk memperoleh *ciphertext* menggunakan persamaan.

$$c = H' \cdot e^T$$

$$= \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Ciphertext c adalah hasil dari sindrom eror terhadap matriks publik H'. Karena Niederreiter bekerja di ruang sindrom, hasil enkripsi memiliki panjang $n - k = 3$ bit, jauh lebih pendek dari pesan aslinya. Namun, tetap aman karena hanya pemilik kunci privat (S, H, P) yang bisa mengembalikan vektor eror e asli dengan algoritma *decoding* BCH.

Proses Dekripsi Pesan

Setelah memperoleh nilai c selanjutnya pada proses dekripsi yang bertujuan untuk mengembalikan vektor kesalahan asli (e) dari *ciphertext* berupa sindrom terenkripsi (c). Setelah penerima menerima *ciphertext.*

$$c = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

Menghitung sindrom terhadap kode BCH dengan menghilangkan efek matriks S, karena S bersifat invertibel.

$$S^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Menghitung sindrom internal (c') yaitu representasi matematis dari posisi kesalahan pada kode.

$$c' = S^{-1} \cdot c$$

$$= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Setelah mendapatkan sindrom c', menentukan vektor kesalahan e dengan menggunakan algoritma *decoding* BCH(7, 4, 1). Proses ini bertujuan untuk menemukan posisi bit yang mengalami kesalahan berdasarkan sindrom. Jika c' yang diterima cocok dengan kolom ke-i pada matriks H, maka berarti bit ke-i pada $H.P$ bernilai 1.

$$H.P = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Dengan demikian, penerima dapat langsung mengidentifikasi posisi kesalahan dengan mencocokan matriks c' sesuai dengan kolom ke-5 pada matriks $H \cdot P$. Maka diperoleh:

$$e' = [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]^T$$

Setelah vektor kesalahan termutasi e' berhasil diperoleh, tahap selanjutnya adalah mengembalikan ke bentuk aslinya dengan mengembalikan efek matriks P. Operasinya dilakukan dengan persamaan:

$$e = P^{-1} \cdot e'$$

$$= \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}^T \quad \rightarrow e = [0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0]$$

Vektor kesalahan e yang diperoleh pada tahap akhir harus sama dengan vektor kesalahan asli yang digunakan saat enkripsi. Vektor e merupakan hasil dekripsi dari pesan rahasia yang sesuai dengan *ciphertext* c.

SIMPULAN

Berdasarkan hasil dan pembahasan yang telah dilakukan, penerapan Kode BCH pada Kriptosistem Niederreiter menunjukkan hasil yang sesuai dengan teori dan perhitungan matematis. Pada proses pembangkitan kunci, diperoleh matriks paritas BCH yaitu H yang berukuran 3×7, matriks acak invertible S berukuran 3×3, dan permutasi P berukuran 7×7. Sedangkan kunci publik menghasilkan matriks H' dengan mengoperasikan $S \cdot H \cdot P$ dan berukuran 3×7.

Pada proses enkripsi, vektor kesalahan e dibentuk sebagai pesan rahasia yang kemudian dienkripsi menjadi *ciphertext* dalam bentuk sindrom $c = H' \cdot e^T$, dimana H' merupakan matriks publik hasil dari $S \cdot H \cdot P$. Proses ini menghasilkan *ciphertext* berdimensi lebih kecil dari pesan asli, namun tetap aman karena hanya pihak yang memiliki kunci privat yang dapat mengembalikannya.

Pada proses dekripsi, penerima menggunakan invers matriks S^{-1} untuk memperoleh sindrom internal $c' = S^{-1} \cdot c$, kemudian melakukan decoding BCH untuk menemukan posisi kesalahan dan memperoleh vektor kesalahan termutasi e'. Setelah efek permutasi dihilangkan menggunakan P^{-1}, diperoleh kembali vektor kesalahan asli e, yang identik dengan vektor saat enkripsi.

Hasil ini, mampu membuktikan bahwa penerapan Kode BCH pada Kriptosistem Niederreiter efektif menjaga kerahasiaan pesan, memiliki mekanisme pemulihan eror yang kuat, serta valid dalam implementasi kunci publik berbasis matriks paritas Kode BCH. Namun demikian, penelitian ini memiliki keterbatasan, yaitu penggunaan parameter BCH dengan ukuran kecil $(7,4,1)$ sehingga belum merepresentasikan kompleksitas sistem pada skala praktis. Selain itu, penelitian ini belum membahas analisis keamanan terhadap serangan kriptanalisis maupun evaluasi efisiensi komputasi untuk parameter yang lebih besar. Oleh karena itu, penelitian selanjutnya disarankan untuk menggunakan parameter BCH yang lebih besar serta melakukan analisis keamanan dan performa sistem secara lebih mendalam.

DAFTAR PUSTAKA

Annechini, A., Barenghi, A., Pelosi, G., & Perriello, S. (2025). Designing QC-MDPC public key encryption schemes with Niederreiter's construction. *IACR Cryptology ePrint Archive*, Paper 2025/1043.

Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). *Post-quantum cryptography*. Springer.

Chusnia, A. L., Khudzaifah, M., & Herawati, E. (2025). Penerapan kriptosistem Niederreiter menggunakan kode Goppa biner untuk mendukung keamanan data dalam sistem kriptografi modern. *Jurnal Riset Mahasiswa Matematika, 4*(3), 133–137.

Davydov, V. V., Beliaev, V. V., Kustov, E. F., Leevik, A. G., & Bezzateev, S. V. (2022). Modern variations of McEliece and Niederreiter cryptosystems. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 22*(2), 324–331.

Fadhilah, R. A. (2022). *Penerapan kode BCH dalam sistem kriptografi kunci publik* [Undergraduate thesis, Universitas Negeri Semarang].

Giorgi, P., Laguillaumie, F., Ottow, L., & Vergnaud, D. (2025). Threshold Niederreiter: Chosen-ciphertext security and improved distributed decoding. *IACR Cryptology ePrint Archive*, Paper 2025/757.

Gorbenko, Y., Kiian, A., Pushkar'ov, A., Korneiko, O., & Smirnov, S. (2024). Code-based hybrid cryptosystem: Comparative studies and analysis of efficiency. *International Journal of Computing, 18*(4), 1608–1617.

Halim, S. K., & Sugeng, K. A. (2024). Application of Goppa code in Niederreiter cryptosystem. In *AIP Conference Proceedings* (Vol. 3163, No. 1).

Hidayah, S. N. (2020). *Analisis performa kode Goppa dan kode BCH pada kriptosistem kunci publik* [Undergraduate thesis, Universitas Airlangga].

Hidayatullah, A. A. (2024). *Implementasi kode BCH (Bose–Chaudhuri–Hocquenghem) pada kriptosistem McEliece*[Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim].

Khalvan, A., Zali, A., & Ahmadian Attari, M. (2023). A tiny public key scheme based on Niederreiter cryptosystem. *arXiv*. https://arxiv.org/abs/2310.06724

Lestari, N. K. (2020). *Analisis keamanan kriptosistem Niederreiter berbasis kode koreksi kesalahan* [Undergraduate thesis, Institut Teknologi Sepuluh Nopember].

Pratama, A. R. (2021). *Implementasi kriptosistem McEliece menggunakan kode BCH* [Undergraduate thesis, Universitas Gadjah Mada].

Sajjad, M., Abid, M. S., Alammari, M., & Serna, R. J. (2025). Structural insights and decoding strategies for BCH codes over quasi-Galois rings. *European Journal of Pure and Applied Mathematics, 18*(3).

Susilowati, D. (2025). *Penerapan generator polinomial untuk optimasi deteksi dan koreksi kesalahan bit pada Bose–Chaudhuri–Hocquenghem code* [Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim].

Sutarto, M., Suwadi, I., & Suryani, I. T. (2014). Implementasi encoder dan decoder BCH menggunakan DSK TMS320C6416T. *Jurnal Teknik POMITS, 3*(1), 29–34.

Utami, R. P. (2023). *Penerapan kode Hamming pada kriptosistem McEliece* [Undergraduate thesis, Universitas Sebelas Maret].

Weger, V., Gassner, N., & Rosenthal, J. (2024). A survey on code-based cryptography. *arXiv*. https://arxiv.org/abs/2201.07119

Widyawati, K. (2024). *Penerapan kode Hamming pada kriptosistem McEliece dan Niederreiter* [Undergraduate thesis, Universitas Sebelas Maret].

Zhang, Y., Liu, H., Wang, X., & Chen, J. (2025). Exploring the landscape of post-quantum cryptography: A bibliometric analysis of emerging trends and research impact. *Journal of Big Data, 12*, Article 225.

Zhao, X., Li, Y., & Wang, H. (2023). New code-based cryptosystems via the IKKR framework. *Journal of Information Security and Applications, 72*, 103344.