Jurnal EurekaMatika

Journal homepage: https://ejournal.upi.edu/index.php/JEM
doi: https://doi.org/10.17509/jem.v13i2.87588

Rekonstruksi Struktur Modul $E_p^{(m)}$ dan Aplikasinya dalam Kriptanalisis Protokol DHDP

*Ridwan Hasyim Umar, Sisilia Sylviani**

Universitas Padjadjaran, Jl. Soekarno Km 21 Jatinangor, Kab.Sumedang, 45363, Indonesia

*Correspondence: sisilia.sylviani@unpad.ac.id

A B S T R A K

Struktur modul atas ring lokal $\mathbb{Z}/p^m\mathbb{Z}$, khususnya modul $E_p^{(m)}$, memberikan pendekatan baru dalam analisis sistem kriptografi berbasis matriks. Dalam konteks keamanan protokol Diffie–Hellman Decomposition Problem (DHDP), pemanfaatan sifat Isomorfisma antara $E_p^{(m)}$ dan submodul $F_p^{(m)} \subseteq \mathrm{Mat}_{m\times m}(\mathbb{Z}/p^m\mathbb{Z})$ memungkinkan reduksi serangan terhadap protokol menjadi sistem persamaan linear biasa. Artikel ini membahas secara sistematik konsep $H(M)$, $\mathrm{Cen}(M)$, serta dua proposisi penting mengenai struktur dan representasi $E_p^{(m)}$, lalu menerapkannya dalam membangun serangan deterministik terhadap DHDP. Hasil menunjukkan bahwa pendekatan ini tidak hanya menyederhanakan proses kriptanalisis, tetapi juga membuka jalur baru dalam desain protokol kriptografi berbasis struktur modul.

© 2025 Kantor Jurnal dan Publikasi UPI

INFORMASI ARTIKEL

Sejarah Artikel:

Diterima 9 Juli 2025
Direvisi 23 Juli 2025
Disetujui 2 September 2025
Tersedia online 2 November 2025
Dipublikasikan 2 November 2025

Kata Kunci:
DHDP,
$E_p^{(m)}$,
$F_p^{(m)}$,
Kriptanalisis,
Struktur modul.

A B S T R A C T

The module structure over local rings, particularly the module $E_p^{(m)}$, offers a novel approach to the analysis of matrix-based cryptographic systems. In the context of the security of the Diffie–Hellman Decomposition Problem (DHDP) protocol, the utilization of an isomorphism between $E_p^{(m)}$ and its submodule $F_p^{(m)}$ enables the reduction of attacks on the protocol to systems of ordinary linear equations. This article systematically discusses the concepts of $H(M)$, $\mathrm{Cen}(M)$, and two key propositions regarding their structure and representation, and then applies these to construct a deterministic attack on DHDP. The findings indicate that this approach not only simplifies the cryptanalysis process but also opens new pathways in the design of cryptographic protocols based on module structures.

© 2025 Kantor Jurnal dan Publikasi UPI

Keywords:
DHDP,
$E_p^{(m)}$,
$F_p^{(m)}$,
Cryptanalysis,
Module structure.

1. PENDAHULUAN

Kemajuan komputasi modern, termasuk ancaman komputasi kuantum, mendorong pengembangan skema kriptografi untuk melawan ancaman dari komputer kuantum masa depan (Khamalwa, 2024; Takagi, 2018; Ustimenko & Pustovit, 2021). Protokol jaringan kriptografi memainkan peran penting dalam memastikan pertukaran data yang aman pada media komunikasi yang tidak aman, namun bahkan kerentanan kecil dapat dimanfaatkan oleh penyerang sehingga analisis terhadap ancaman dan kelemahan protokol ini menjadi sangat krusial (Ahn, *et al*., 2024). Berbagai pendekatan telah diusulkan, salah satunya adalah dengan memanfaatkan masalah komputasi yang sulit dalam struktur aljabar non-komutatif (Ustimenko & Woldar, 2019; Grover, *et al*.,2022). Pengembangan protokol kriptografi seringkali berfokus pada penggunaan struktur non-komutatif untuk menghindari serangan yang berlaku pada sistem komutatif (Selikh, *et al*., 2024). Struktur-struktur seperti ring grup hingga semi-ring, menawarkan platform alternatif untuk membangun protokol kriptografi yang aman (Hanoymak & Küsmüş, 2019). Meskipun demikian, banyak dari protokol ini kemudian terbukti rentan, terutama yang berbasis semi-ring tropis, yang sebagian besar telah berhasil dipecahkan (Durcheva, 2025).

Salah satu struktur yang menonjol dalam pendekatan ini adalah ring matriks $E_p^{(m)}$, yaitu himpunan matriks berukuran $m \times m$ dengan entri-entri yang mengikuti pola khusus berdasarkan pangkat lokal dari bilangan prima p. Pemanfaatan aksi sebuah ring pada suatu modul dapat digunakan untuk membangun generalisasi dari protokol Diffie-Hellman dan ElGamal (Maze, et al., 2002; Ghadafi, 2017). Struktur $E_p^{(\mathrm{m})}$ memiliki keunikan karena tidak menyematkan dirinya sebagai subring dari ring matriks biasa di atas suatu lapangan, melainkan merupakan ring dengan properti lokal tertentu yang menghasilkan kompleksitas tinggi dalam analisis langsung.

Namun, setiap usulan kriptografi baru harus diuji ketahanannya terhadap berbagai teknik kriptanalisis. Sejarah telah menunjukkan bahwa banyak skema pertukaran kunci yang sebelumnya dianggap aman ternyata tidak aman setelah ditemukan serangan yang mampu mengungkap kunci rahasia hanya dari informasi publik (Sánchez & Ramos, 2024). Analisis keamanan seringkali berhasil membuktikan adanya kelemahan fatal yang membuat sebuah protokol tidak aman, seperti serangan peniruan identitas (Hatri, *et al.*, 2017). Hasil penelitian matematis yang dilakukan oleh (Khathuria et al., 2021) menunjukkan bahwa $E_p^{(\mathrm{m})}$, sebagai modul atas $\mathbb{Z}/p^m\mathbb{Z}$, ternyata isomorfik dengan suatu submodul $F_p^{(m)} \subseteq \mathrm{Mat}_{m\times m}(\mathbb{Z}/p^m\mathbb{Z})$. Isomorfisma ini memungkinkan konversi persoalan dalam $E_p^{(m)}$ ke dalam konteks linear yang lebih mudah dianalisis secara algoritmik, sebuah pendekatan yang sering dicari dalam kriptanalisis (Dubois & Kammerer, 2011). Kemudian, penelitian (Khathuria *et al*., 2021) berhasil memperlihatkan celah keamanan pada protokol Diffie–Hellman *Decomposition Problem* (DHDP). Kontribusi utama mereka adalah menunjukkan bahwa serangan terhadap protokol ini dapat direduksi ke sistem persamaan linear homogen dalam $\mathbb{Z}/p^m\mathbb{Z}$, yang dapat diselesaikan secara efisien dalam kompleksitas waktu $\mathcal{O}(m^6)$.

Artikel ini bertujuan untuk menguraikan kembali dan memberikan verifikasi numerik terhadap metode serangan yang mereka kembangkan. Artikel ini memperluas hasil tersebut dengan menyusun ulang struktur pusat $\mathrm{Cen}(M)$, submodul $H(M)$, serta dua proposisi penting yang menunjukkan bahwa representasi elemen $GA = A_1XA_2$ dalam protokol DHDP dapat ditulis sebagai kombinasi linear dari matriks M^iXM^j, dan bahwa $E_p(m) \cong F_p(m)$ sebagai $\mathbb{Z}/p^m\mathbb{Z}$-modul. Kebaruan dari artikel ini terletak pada:

a. Penjabaran ulang yang lebih eksplisit dan terstruktur terhadap struktur aljabar $E_p^{(m)}$ sebagai modul, serta bentuk umum dari GA.
b. Penyusunan langkah-langkah serangan DHDP berbasis representasi linier dengan pembuktian ulang terhadap proposisi 1 dan 2 dari (Khathuria *et al*., 2021).
c. Pemberian contoh numerik lengkap dan verifikasi hasil serangan terhadap protokol DHDP tanpa memerlukan informasi rahasia, yang ditulis dengan pendekatan instruktif dan mudah direplikasi.

Dengan demikian, pendekatan ini tidak hanya menyederhanakan proses kriptanalisis, tetapi juga membuka jalur baru dalam desain protokol kriptografi berbasis struktur modul.

2. METODE

Pendekatan yang digunakan dalam artikel ini melibatkan kajian teoretis terhadap definisi dan struktur internal dari $E_p^{(m)}$, termasuk penurunan Isomorfisma modul, serta penerapan struktur tersebut dalam konteks serangan terhadap protokol kriptografi. Langkah-langkah utama yang dilakukan meliputi:

a. Menyusun ulang definisi dari $E_p^{(m)}$, yaitu ring matriks dengan entri-entri yang berada pada kongruensi modulo p^i, dan mendeskripsikan submodul $F_p^{(m)}$ sebagai himpunan matriks dengan entri-entri kelipatan tertentu dari p.
b. Mendefinisikan dan menganalisis pusat dari suatu matriks M dalam $E_p^{(m)}$, yang dilambangkan dengan $\mathrm{Cen}(M)$, serta submodul $H(M)$, yang dibentuk dari kombinasi polinomial terhadap M.
c. Menyusun ulang dan membuktikan kembali dua proposisi penting:
   - Proposisi 1 pada (Khathuria *et al*., 2021), yang menjelaskan bahwa setiap matriks dari bentuk A_1XA_2, dengan $A_1, A_2 \in H(M)$, dapat diekspresikan sebagai kombinasi linear dari M^iXM^j dengan koefisien dalam $\mathbb{Z}/p^m\mathbb{Z}$.
   - Proposisi 2 pada (Khathuria et al., 2021), yang menjelaskan bahwa terdapat Isomorfisma modul antara $E_p^{(m)}$ dan $F_p^{(m)}$, yang memungkinkan pemetaan langsung ke dalam bentuk homogen.
d. Membangun ulang prosedur serangan terhadap protokol DHDP berdasarkan representasi di atas, kemudian menyimulasikan penerapannya secara numerik pada contoh sederhana.

Metode ini bersifat konstruktif dan bertujuan membangun pemahaman menyeluruh dari definisi dasar hingga implementasi serangan.

3. HASIL DAN PEMBAHASAN

3.1 Struktur Modul $E_p^{(m)}$ dan Submodul $F_p^{(m)}$

Struktur ring $E_p^{(m)}$ terdiri atas matriks berukuran $m \times m$ dengan entri-entri a_{ij} yang dibangun sebagai berikut:

$$E_p^{(m)} = \left\{ (a_{ij}) \in \mathrm{Mat}_{m\times m} \;\middle|\; \begin{cases} a_{ij} \in \mathbb{Z}/p^i\mathbb{Z}, & \text{jika } i \le j, \\ a_{ij} \in p^{i-j}\mathbb{Z}/p^i\mathbb{Z}, & \text{jika } i > j \end{cases} \right\}.$$

Secara umum, struktur matriks $E_p^{(m)}$ berbentuk:

$$E_p^{(m)} = \begin{bmatrix} \mathbb{Z}/p^1 & \mathbb{Z}/p^1 & \cdots & \mathbb{Z}/p^1 \\ p\mathbb{Z}/p^2 & \mathbb{Z}/p^2 & \cdots & \mathbb{Z}/p^2 \\ \vdots & \vdots & \ddots & \vdots \\ p^{m-1}\mathbb{Z}/p^m & p^{m-2}\mathbb{Z}/p^m & \cdots & \mathbb{Z}/p^m \end{bmatrix}$$

Karena setiap baris memiliki modulus berbeda, maka ring ini tidak homogen secara modul, sehingga sulit diterapkan langsung untuk penyelesaian sistem linear. Sebagai solusi, dibentuk submodul $F_p^{(m)} \subseteq \text{Mat}_{m\times m}(\mathbb{Z}/p^m\mathbb{Z})$ dengan entri-entri sebagai berikut:

$$F_p^{(m)} = \left\{(a_{ij}) \in \text{Mat}_{m\times m} \;\middle|\; a_{ij} \in p^{\max(m-i,m-j)}\mathbb{Z}/p^m\mathbb{Z}\right\}.$$

Secara umum, bentuk struktur matriks $F_p^{(m)}$ adalah:

$$F_p^{(m)} = \begin{bmatrix} p^{m-1} & p^{m-1} & \cdots & p^{m-1} \\ p^{m-2} & p^{m-2} & \cdots & p^{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{bmatrix} \cdot \mathbb{Z}/p^m\mathbb{Z}$$

Submodul ini homogen terhadap $\mathbb{Z}/p^m\mathbb{Z}$, sehingga mendukung penyelesaian sistem linear standar. Hubungan antara $E_p^{(m)}$ dan $F_p^{(m)}$ dijembatani oleh suatu pemetaan isomorfik modul sebagai berikut:

$$\delta: E_p^{(m)} \to F_p^{(m)}, \quad \delta((a_{ij})) = (a_{ij} \cdot p^{m-i}) \bmod p^m.$$

3.2 Pembuktian Isomorfisma Modul

Berikut ini ditunjukkan bahwa δ adalah Isomorfisma $\mathbb{Z}/p^m\mathbb{Z}$-modul.

i. *Well-defined*

Misalkan $A = (a_{ij}) \in E_p^{(m)}$. Untuk setiap entri a_{ij}, berlaku:

- Jika $i \le j$: $a_{ij} \in \mathbb{Z}/p^i\mathbb{Z} \Rightarrow a_{ij} \cdot p^{m-i} \in \mathbb{Z}/p^m\mathbb{Z}$.
- Jika $i > j$: $a_{ij} \in p^{i-j}\mathbb{Z}/p^i\mathbb{Z} \Rightarrow a_{ij} \cdot p^{m-i} \in p^{m-j}\mathbb{Z}/p^m\mathbb{Z}$.

Jadi setiap entri hasil $\delta(A)$ berada pada posisi yang sesuai dalam $F_p^{(m)}$. Dengan kata lain, δ terdefinisi dengan baik.

ii. Aditif

Misalkan $A = (a_{ij}), B = (b_{ij}) \in E_p^{(m)}$, maka:

$$\delta(A + B) = ((a_{ij} + b_{ij}) \cdot p^{m-i}) = a_{ij} \cdot p^{m-i} + b_{ij} \cdot p^{m-i} = \delta(A) + \delta(B).$$

Dengan kata lain, δ aditif.

iii. Homogen terhadap skalar

Untuk $r \in \mathbb{Z}/p^m\mathbb{Z}$, dan $A = (a_{ij}) \in E_p^{(m)}$, berlaku:

$$\delta(r \cdot A) = (r \cdot a_{ij} \cdot p^{m-i}) = r \cdot (a_{ij} \cdot p^{m-i}) = r \cdot \delta(A).$$

Dengan kata lain, δ homogen terhadap skalar.

iv. Injektif

Misalkan $\delta(A) = \delta(B)$, hal ini berarti

$$a_{ij} \cdot p^{m-i} \equiv b_{ij} \cdot p^{m-i} \bmod p^m.$$

Lebih lanjut, karena p^{m-i} tidak nol dalam $\mathbb{Z}/p^m\mathbb{Z}$ akibatnya

$$a_{ij} \equiv b_{ij} \bmod p^i.$$

Karena $a_{ij}, b_{ij} \in \mathbb{Z}/p^i\mathbb{Z}$, maka $a_{ij} = b_{ij}$, atau dengan kata lain $A = B$, sehingga δ injektif.

v. Surjektif

Misalkan $B = (b_{ij}) \in F_p^{(m)}$, maka untuk setiap i, j, terdapat:

$$b_{ij} \in p^{\max(m-i,m-j)}\mathbb{Z}/p^m\mathbb{Z}.$$

Definisikan $a_{ij} = b_{ij} \cdot p^{i-m} \bmod p^i$.

- Jika $i \leq j$, maka $b_{ij} \in p^{m-i} \Rightarrow a_{ij} \in \mathbb{Z}/p^i$.
- Jika $i > j$, maka $b_{ij} \in p^{m-j} \Rightarrow a_{ij} \in p^{i-j}\mathbb{Z}/p^i$.

Sehingga, $A = (a_{ij}) \in E_p^{(m)}$ dan $\delta(A) = B$. Terbukti bahwa δ surjektif. Dengan demikian, karena δ memenuhi kelima syarat sebagai pemetaan modul—*well-defined*, aditif, homogen, injektif, dan surjektif—maka δ adalah Isomorfisma $\mathbb{Z}/p^m\mathbb{Z}$-modul:

$$E_p^{(m)} \cong F_p^{(m)}.$$

3.3 Struktur Cen(M) dan $H(M)$

Diberikan $M \in E_p^{(m)}$, maka:

- Pusat dari M didefinisikan sebagai himpunan:
$$\text{Cen}(M) = \{X \in E_p^{(m)} \mid XM = MX\}.$$
- Subaljabar $H(M)$ adalah himpunan:
$$H(M) = \left\{\sum_{i=0}^{k} C_i M^i \;\middle|\; C_i \in Z(E_p^{(m)}), k \in \mathbb{N}\right\},$$

di mana $Z(E_p^{(m)}) \cong \mathbb{Z}/p^m\mathbb{Z}$ adalah pusat dari ring. Kedua struktur ini memiliki peran penting dalam protokol DHDP:

- Elemen-elemen rahasia milik Siti diambil dari $H(M)$,
- Elemen-elemen rahasia milik Nimo diambil dari Cen(M),
- Syarat $M \notin \text{Cen}(X)$ memastikan bahwa komutator tidak trivial, menjaga keamanan protokol.

3.4 Bentuk Umum GA dan Reduksi Linear

Proposisi 1. Berdasarkan Khathuria et al., (2021), jika $A_1, A_2 \in H(M)$, maka:

$$GA = A_1XA_2 = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} \lambda_{ij} M^i X M^j, \quad \lambda_{ij} \in \mathbb{Z}/p^m\mathbb{Z}.$$

Hal tersebut mempunyai makna GA dapat direpresentasikan sebagai kombinasi linear dari m^2 matriks dasar M^iXM^j. Vektor koefisien (λ_{ij}) inilah yang menjadi target serangan.

3.5 Algoritma Serangan DHDP Berdasarkan Isomorfisma Modul

Setelah Isomorfisma antara $E_p^{(m)}$ dan $F_p^{(m)}$ dibuktikan, kemudian isomorfisma modul tersebut digunakan untuk merumuskan kembali protokol DHDP dalam bentuk sistem persamaan linear atas $\mathbb{Z}/p^m\mathbb{Z}$. Ini memungkinkan serangan deterministik terhadap protokol tanpa memerlukan informasi rahasia.

Protokol DHDP melibatkan dua pihak, misalnya Siti dan Nimo, yang menyepakati dua elemen publik $M, X \in E_p^{(m)}$ dengan syarat $MX \neq XM$. Protokol bekerja sebagai berikut:

1. Siti memilih $S_1, S_2 \in H(M)$ dan mengirim $GS = S_1XS_2$.
2. Nimo memilih $N_1, N_2 \in \text{Cen}(M)$ dan mengirim $GB = N_1XN_2$.
3. Informasi rahasia diperoleh Siti dengan menghitung S_1GBS_2, dan Nimo menghitung N_1GAN_2.

4. Keduanya memperoleh nilai bersama yang sama.

Serangan terhadap DHDP dilakukan dalam langkah berikut:

1. Input Diketahui Umum
   $M, X, GS = S_1XS_2, GB = N_1XN_2$, dengan $S_1, S_2 \in H(M)$ dan $N_1, N_2 \in \text{Cen}(M)$.
2. Membangun Matriks Basis
   Berdasarkan proposisi 1 (Khathuria et al., 2021), diketahui bahwa jika $S_1, S_2 \in H(M)$, maka:
   $$GS = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \lambda_{ij} M^i X M^j$$
   dengan $\lambda_{ij} \in \mathbb{Z}/p^m\mathbb{Z}$.
3. Mengkonversi ke Modul Homogen dengan Isomorfisma
   Matriks-matriks dalam $E_p^{(m)}$ memiliki entri dengan modulus yang bervariasi per baris (tidak homogen), sehingga sulit diperlakukan seperti sistem linear biasa. Karena itu digunakan Isomorfisma δ dari Proposisi 2 (Khathuria *et al*., 2021):
   $$\delta: E_p^{(m)} \to F_p^{(m)}, \quad \delta((a_{ij})) = (a_{ij} \cdot p^{m-i}) \bmod p^m$$
   Pemetaan ini membawa matriks dari struktur bercampur ke bentuk homogen dalam $\text{Mat}_{m\times m}(\mathbb{Z}/p^m\mathbb{Z})$, sehingga dapat digunakan untuk menyusun sistem linear.
4. Membentuk Sistem Linier
   Dibentuk sistem linier:
   $$\delta(GS) = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \lambda_{ij} \cdot \delta\left(M^i X M^j\right).$$
   Selanjutnya sistem tersebut diselesaikan untuk mendapatkan λ_{ij}.
5. Merekonstruksi Rahasia
   Rekonstruksi:
   $$S_1 GB S_2 = \sum_{i,j} \lambda_{ij} M^i GB M^j,$$
   dan menghitung hasilnya sebagai kunci bersama tanpa mengetahui S_1, S_2, N_1, N_2.

Langkah-langkah ini bersifat deterministik dan dapat dijalankan dalam kompleksitas $\mathcal{O}(m^6)$ operasi di $\mathbb{Z}/p^m\mathbb{Z}$ (Khathuria *et al*., 2021).

3.6 Contoh Penerapan Serangan DHDP secara Numerik

Sebagai ilustrasi, digunakan parameter $p = 7$ dan $m = 2$, sehingga $p^m = 49$. Ring modulusnya adalah $\mathbb{Z}/49\mathbb{Z}$. Matriks dalam $E_7^{(2)}$ berbentuk $\begin{pmatrix} a_{11} \in \mathbb{Z}/7\mathbb{Z} & a_{12} \in \mathbb{Z}/7\mathbb{Z} \\ a_{21} \in 7\mathbb{Z}/49\mathbb{Z} & a_{22} \in \mathbb{Z}/49\mathbb{Z} \end{pmatrix}$.

- **Inisialisasi Publik**

  Misalkan Siti dan Nimo menyetujui matriks publik: $M = \begin{pmatrix} 1 & 2 \\ 7 & 3 \end{pmatrix}, X = \begin{pmatrix} 4 & 5 \\ 0 & 6 \end{pmatrix}$.

- **Pertukaran Kunci:**

  1) Siti memilih kunci rahasia $S_1 = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$, $S_2 = \begin{pmatrix} 4 & 2 \\ 7 & 6 \end{pmatrix}$ dan menghitung $G_S = S_1XS_2 = \begin{pmatrix} 6 & 4 \\ 28 & 5 \end{pmatrix}$.

2) Nimo memilih kunci rahasia $N_1 = \begin{pmatrix} 3 & 4 \\ 14 & 7 \end{pmatrix}$, $N_2 = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$ dan menghitung $G_N = N_1 X N_2 = \begin{pmatrix} 1 & 2 \\ 21 & 35 \end{pmatrix}$.
3) Penyerang melihat M, X, G_S, G_S, tujuannya adalah mencari $R = S_1 G_B S_2$.

- **Langkah Serangan oleh penyerang:**

a. Menyusun Persamaan: Penyerang berasumsi $G_S = \lambda_{00} X + \lambda_{01} XM + \lambda_{10} MX + \lambda_{11} MXM$. Penyerang perlu menghitung matriks komponen $M^i X M^j$: $X = \begin{pmatrix} 4 & 5 \\ 0 & 6 \end{pmatrix}$ $XM = \begin{pmatrix} 4 & 2 \\ 42 & 18 \end{pmatrix}$ $MX = \begin{pmatrix} 4 & 3 \\ 28 & 4 \end{pmatrix}$ $MXM = \begin{pmatrix} 4 & 3 \\ 7 & 19 \end{pmatrix}$

b. Menerapkan Isomorfisma δ**:** Pemetaan δ untuk $m = 2$ adalah $\delta\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a \cdot 7^{2-1} & b \cdot 7^{2-1} \\ c \cdot 7^{2-2} & d \cdot 7^{2-2} \end{bmatrix} = \begin{bmatrix} 7a & 7b \\ c & d \end{bmatrix} \pmod{49}$.
Penyerang menerapkan δ pada semua matriks: $\delta(G_S) = \begin{pmatrix} 42 & 28 \\ 28 & 5 \end{pmatrix}$ $\delta(X) = \begin{pmatrix} 28 & 35 \\ 0 & 6 \end{pmatrix}$ $\delta(XM) = \begin{pmatrix} 28 & 14 \\ 42 & 18 \end{pmatrix}$ $\delta(MX) = \begin{pmatrix} 28 & 21 \\ 28 & 4 \end{pmatrix}$ $\delta(MXM) = \begin{pmatrix} 28 & 21 \\ 7 & 19 \end{pmatrix}$

c. Memecahkan Sistem Persamaan Linear: Penyerang menyusun persamaan matriks $\delta(G_S) = \lambda_{00}\delta(X) + \lambda_{01}\delta(XM) + \lambda_{10}\delta(MX) + \lambda_{11}\delta(MXM)$ di $\mathbb{Z}/49\mathbb{Z}$. Ini menghasilkan 4 persamaan linear dengan 4 variabel:
   - $42 = 28\lambda_{00} + 28\lambda_{01} + 28\lambda_{10} + 28\lambda_{11}$
   - $28 = 35\lambda_{00} + 14\lambda_{01} + 21\lambda_{10} + 21\lambda_{11}$
   - $28 = 0\lambda_{00} + 42\lambda_{01} + 28\lambda_{10} + 7\lambda_{11}$
   - $5 = 6\lambda_{00} + 18\lambda_{01} + 4\lambda_{10} + 19\lambda_{11}$

   Salah satu solusi untuk sistem ini (mod 49) adalah: $\lambda_{00} = 6, \lambda_{01} = 2, \lambda_{10} = 3, \lambda_{11} = 1$. Solusi diverifikasi, yaitu sebagai berikut:
   i. $28(6) + 28(2) + 28(3) + 28(1) = 168 + 56 + 84 + 28 = 336 \equiv 42 \pmod{49}$. (Benar)
   ii. $35(6) + 14(2) + 21(3) + 21(1) = 210 + 28 + 63 + 21 = 322 \equiv 28 \pmod{49}$. (Benar)
   iii. $42(2) + 28(3) + 7(1) = 84 + 84 + 7 = 175$ $175 \equiv 28 \pmod{49}$. (Benar)
   iv. $6(6) + 18(2) + 4(3) + 19(1) = 36 + 36 + 12 + 19 = 103 \equiv 5 \pmod{49}$. (Benar)

d. Merekonstruksi Kunci Rahasia: Penyerang sekarang dapat menghitung kunci bersama S tanpa mengetahui kunci rahasia S_1, S_2, N_1 atau N_2 menggunakan $R = S_1 G_N S_2 = \sum_{i,j} \lambda_{ij} M^i G_N M^j$.
   $R = 6G_N + 2G_N M + 3MG_N + 1MG_N M$ Penyerang melakukan perhitungan:
   - $G_N = \begin{pmatrix} 1 & 2 \\ 21 & 35 \end{pmatrix}$
   - $G_N M = \begin{pmatrix} 15 & 8 \\ 266 & 147 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 21 & 0 \end{pmatrix}$
   - $MG_N = \begin{pmatrix} 43 & 72 \\ 70 & 119 \end{pmatrix} = \begin{pmatrix} 43 & 23 \\ 21 & 21 \end{pmatrix}$
   - $MG_N M = \begin{pmatrix} 15 & 8 \\ 168 & 105 \end{pmatrix} = \begin{pmatrix} 15 & 8 \\ 21 & 7 \end{pmatrix}$

   Substitusikan ke dalam rumus R:
   $$R = 6\begin{pmatrix} 1 & 2 \\ 21 & 35 \end{pmatrix} + 2\begin{pmatrix} 1 & 1 \\ 21 & 0 \end{pmatrix} + 3\begin{pmatrix} 43 & 23 \\ 21 & 21 \end{pmatrix} + 1\begin{pmatrix} 15 & 8 \\ 21 & 7 \end{pmatrix}$$

$$R = \begin{pmatrix} 6 & 12 \\ 126 & 210 \end{pmatrix} + \begin{pmatrix} 2 & 2 \\ 42 & 0 \end{pmatrix} + \begin{pmatrix} 129 & 69 \\ 63 & 63 \end{pmatrix} + \begin{pmatrix} 15 & 8 \\ 21 & 7 \end{pmatrix}$$
$$R = \begin{pmatrix} 6+2+129+15 & 12+2+69+8 \\ 126+42+63+21 & 210+0+63+7 \end{pmatrix}$$

Entri a_{11} dan a_{12} dihitung mod 7, sedangkan a_{21} dan a_{22} dihitung mod 49.

$$R = \begin{pmatrix} 152 & 91 \\ 252 & 280 \end{pmatrix} = \begin{pmatrix} 152 \pmod 7 & 91 \pmod 7 \\ 252 \pmod{49} & 280 \pmod{49} \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 7 & 35 \end{pmatrix}$$

Penyerang berhasil mendapatkan kunci bersama $R = \begin{pmatrix} 5 & 0 \\ 7 & 35 \end{pmatrix}$ tanpa mengetahui rahasia Siti dan Nimo. Untuk mengonfirmasi validitas dan keakuratan serangan yang dilakukan oleh Penyerang, dilakukan perhitungan kunci rahasia bersama dari sudut pandang Siti. Kemudian, Siti akan menggunakan kunci privatnya (S_1 dan S_2) dan kunci publik Nimo (G_N) untuk menghitung nilai R. Perhitungan yang dilakukan Siti adalah: $R = S_1 G_N S_2$. Dengan matriks yang diketahui dari sebelumnya: $S_1 = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$, $G_N = \begin{pmatrix} 1 & 2 \\ 21 & 35 \end{pmatrix}$, dan $S_2 = \begin{pmatrix} 4 & 2 \\ 7 & 6 \end{pmatrix}$.

Langkah 1: Hitung produk antara G_N dan S_2 Misalnya kita mulai dengan mengalikan G_N dengan S_2.

$$G_N S_2 = \begin{pmatrix} 1 & 2 \\ 21 & 35 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 7 & 6 \end{pmatrix} = \begin{pmatrix} (1 \cdot 4 + 2 \cdot 7) \pmod 7 & (1 \cdot 2 + 2 \cdot 6) \pmod 7 \\ (21 \cdot 4 + 35 \cdot 7) \pmod{49} & (21 \cdot 2 + 35 \cdot 6) \pmod{49} \end{pmatrix}$$
$$= \begin{pmatrix} 18 \pmod 7 & 14 \pmod 7 \\ 329 \pmod{49} & 252 \pmod{49} \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 35 & 7 \end{pmatrix}$$

Langkah 2: Hitung produk antara A_1 dan hasil dari Langkah 1. Selanjutnya, kita mengalikan S_1 dengan matriks hasil $G_N S_2$.

$$R = S_1(G_N S_2) = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} 4 & 0 \\ 35 & 7 \end{pmatrix}$$
$$= \begin{pmatrix} (3 \cdot 4 + 2 \cdot 35) \pmod 7 & (3 \cdot 0 + 2 \cdot 7) \pmod 7 \\ (7 \cdot 4 + 5 \cdot 35) \pmod{49} & (7 \cdot 0 + 5 \cdot 7) \pmod{49} \end{pmatrix}$$
$$= \begin{pmatrix} 82 \pmod 7 & 14 \pmod 7 \\ 203 \pmod{49} & 35 \pmod{49} \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 7 & 35 \end{pmatrix}$$

Hasil Perbandingan

- Kunci rahasia yang dihitung oleh penyerang adalah $R_{penyerang} = \begin{pmatrix} 5 & 0 \\ 7 & 35 \end{pmatrix}$.
- Kunci rahasia yang dihitung oleh Siti adalah $R_{Siti} = \begin{pmatrix} 5 & 0 \\ 7 & 35 \end{pmatrix}$.

Hasil kedua perhitungan adalah identik. Ini secara konkret memverifikasi bahwa metode serangan dengan memanfaatkan Isomorfisma modul berhasil merekonstruksi kunci rahasia bersama dengan benar, meskipun penyerang sama sekali tidak mengetahui kunci-kunci privat yang digunakan oleh Siti (S_1, S_2) dan Nimo (N_1, N_2).

Sebagai catatan, keberhasilan deterministik dari serangan ini bergantung pada sifat sistem persamaan linear yang dibentuk. Jika sistem menghasilkan banyak solusi untuk koefisien λ_{ij} yang mengarah pada rekonstruksi kunci akhir yang berbeda, maka penyerang tidak dapat memastikan kebenaran kunci yang diperoleh. Namun, seperti yang ditunjukkan di (Khathuria et al., 2021), dan diverifikasi dalam contoh numerik kami, serangan ini dapat mereduksi masalah ke sistem linear yang dapat diselesaikan secara efisien, yang secara implisit menunjukkan bahwa untuk parameter yang umum, solusi yang valid dapat ditemukan.

4. KESIMPULAN

Dalam artikel ini telah dibahas bagaimana struktur modul $E_p^{(m)}$ dan Isomorfismanya terhadap submodul $F_p^{(m)}$ dapat dimanfaatkan secara efektif dalam analisis dan serangan terhadap protokol Diffie–Hellman Decomposition Problem (DHDP). Pemetaan δ dari $E_p^{(m)}$ ke $F_p^{(m)}$ menjadi alat fundamental dalam menyederhanakan struktur modul tak homogen menjadi bentuk homogen, sehingga memungkinkan implementasi algoritma serangan linier secara efisien. Hasil dari serangan ini menunjukkan bahwa protokol DHDP yang dibangun di atas $E_p^{(m)}$ dapat direduksi ke sistem linier biasa dalam waktu polinomial, khususnya $\mathcal{O}(m^6)$, sehingga menurunkan keamanan yang diharapkan dari protokol tersebut (Khathuria, *et al*., 2021). Meskipun banyak kriptosistem dirancang dengan ruang kunci yang besar dan keamanan yang bersandar pada masalah yang diyakini sulit seperti DLP (Kumari & Tanti, 2022) atau *Semigroup Action Problem* (SAP) (Atani, *et al*., 2007), celah pada level struktur aljabar tetap dapat muncul. Keamanan sebuah sistem tidak hanya bergantung pada non-komutativitasnya, tetapi juga pada resistensinya terhadap reduksi ke masalah yang lebih mudah, seperti *word problem* (Ustimenko, 2018). Dengan demikian, penggunaan ring $E_p^{(m)}$ dalam sistem kriptografi perlu dikaji ulang dari sisi resistensinya terhadap serangan berbasis struktur modul. Ke depan, desain sistem kriptografi berbasis ring nonkomutatif perlu mempertimbangkan bukan hanya kompleksitas struktur algebraiknya, tetapi juga kemungkinan adanya transformasi linier yang membuka celah kriptanalitik.

5. DAFTAR PUSTAKA

Ahn, J., Hussain, R., Kang, K., & Son, J. (2025). Exploring encryption algorithms and network protocols: a comprehensive survey of threats and vulnerabilities. *IEEE Communications Surveys & Tutorials, 27*(5), 2765-2792.

Atani, R. E., Atani, S. E., & Mirzakuchaki, S. (2009). A novel public key crypto system based on semi-modules over quotient semi-rings. *Journal of Applied Mathematics and Computing, 30*(2), 237-248.

Dubois, V., & Kammerer, J. (2011). Cryptanalysis of cryptosystems based on non-commutative skew polynomials. *Journal of Symbolic Computation*, *46*(3), 355-371.

Durcheva, M. (2025). Cryptography based on (idempotent) semirings: abandoning tropicality?. *Encyclopedia*, *5*(1), 1-20.

Ghadafi, E. (2017). How low can you go? short structure-preserving signatures for Diffie-Hellman vectors. *Proceedings of the IMA International Conference on Cryptography and Coding 2017*. Springer, 1-19.

Grover, C., Mendelsohn, A., Ling, C., et al. (2022). Non-commutative ring learning with errors from cyclic algebras. *Journal of Cryptology*, *35*(3), 1-67.

Hanoymak, T., & Küsmüş, Ö. (2019). A new multi-party key exchange protocol and symmetric key encryption scheme over non-commutative group rings. *Journal of Advances in Mathematics*, *8*(1), 11–16.

Hatri, Y., Otmani, A., & Guenda, K. (2018). Cryptanalysis of an identity-based authenticated key exchange protocol. *Designs, Codes and Cryptography*, *86*(11), 2445-2458.

Kamal, A. A., & Youssef, A. M. (2012). Cryptanalysis of a key exchange protocol based on the endomorphisms ring End $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *Applicable Algebra in Engineering, Communication and Computing*, *23*(3), 143–149.

Khamalwa, M. S. (2024). Exploring how commutative algebra underpins cryptographic protocols and encryption methods used in secure communications and data protection. *Newport International Journal of Scientific and Experimental Sciences*, *5*(3), 58–62.

Khathuria, K., Micheli, G., & Weger, V. (2021). On the algebraic structure of $E_p^{(m)}$ and applications to cryptography. *Applicable Algebra in Engineering, Communication and Computing*, *32*(4), 495–505.

Kumari, M., & Tanti, J. (2022). A public key cryptography using multinacci block matrices. *Sādhanā*, *47*(1), 1-13.

Maze, G., Monico, C., Rosenthal, J., & Climent, J. J. (2004). Public key cryptography based on simple modules over simple rings. *Designs, Codes and Cryptography*, *32*(3), 213-225.

Selikh, B., Chillali, A., Mihoubi, D., & Ghadbane, N. (2024). A new public key cryptosystem based on the non-commutative ring R. *Journal of Discrete Mathematical Sciences & Cryptography*, *27*(1), 75–93.

Takagi, T. (2018). Recent developments in post-quantum cryptography, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E101A(1), 3–11.

Ustimenko, V. A. (2018). On new symbolic key exchange protocols and cryptosystems based on a hidden tame homomorphism. *Dopovidi Nacional'noi Akademii Nauk Ukraini*, (10), 26–36.

Ustimenko, V., & Pustovit, O. (2021). New cryptosystems of noncommutative cryptography based on eulerian semigroups of multivariate transformations. *CEUR Workshop Proceedings*, 2923, 18–26.

Ustimenko, V. A., & Woldar, A. N. (2019). Finite non-commutative associative algebras as carriers of hidden discrete logarithm problem. *Bulletin of the South Ural State University. Series: Mathematics, Mechanics, Computer Science*, *12*(1), 66–75.