**A-11**

# SKEMA PEMBAGIAN RAHASIA DENGAN KODE LINEAR

**Riningsih[1], Indah Emilia Wijayanti[2]**

*[1]Mahasiswa S1 Jurusan Matematika FMIPA Universitas Gadjah Mada*
*[2]Jurusan Matematika FMIPA Universitas Gadjah Mada*

**Abstrak**

Skema pembagian rahasia dikembangkan secara terpisah oleh Shamir dan Blakely pada tahun 1979. Sejak saat itu perkembangan skema pembagian rahasia menjadi sangat pesat. Kebanyakan dari skema adalah sistem (n,k) threshold. Pada makalah ini akan dibahas mengenai skema pembagian rahasia dengan menggunakan kode linear yang diperkenalkan oleh Massey serta beberapa hal yang terkait antara lain codeword minimal, himpunan akses minimal, dan struktur akses.

**Kata kunci**: skema pembagian rahasia, kode linear, codeword minimal, himpunan akses minimal, struktur akses

## PENDAHULUAN

Dalam struktur Aljabar, dikenal sejumlah struktur himpunan yang dilengkapi dengan operasi biner, antara lain adalah grup, gelanggang, lapangan, dan ruang vektor. Dalam sejumlah kasus khusus, terdapat lapangan yang elemennya berhingga. Dalam perkembangannya, banyak aplikasi yang menggunakan ruang vektor atas lapangan hingga. Sebagai contohnya dalam teori pengkodean.

Metode pembagian kunci rahasia menjadi suatu hal yang penting dalam beberapa persoalan keamanan. Banyak faktor yang melatarbelakangi penggunaan metode pembagian rahasia. Faktor kepercayaan individu serta faktor kealpaan manusia menjadi sebab pentingnya penggunaan metode ini. Skema pembagian rahasia menggunakan kode linear adalah salah satu metode terapan dari metode pembagian rahasia.

Konsep dasar skema pembagian rahasia secara sederhana dapat digambarkan sebagai berikut, diberikan kunci K, sebagai data rahasia. Kemudian kunci $K$ dibagi-bagi menjadi beberapa bagian misalkan 5 bagian, $a, b, c, d,$ dan $e$, sehingga dapat ditulis $\mathrm{K} = \mathrm{a} + \mathrm{b} + \mathrm{c} + \mathrm{d} + \mathrm{e}$. Untuk mendapatkan nilai $K$ kembali, maka masing-masing bagian dari $a, b, c, d,$ dan $e$ harus dikumpulkan dan direkonstruksikan lagi sehingga didapatkan kunci $K$. Jika ada satu bagian yang hilang, maka kunci $K$ mustahil untuk didapatkan. Pada implementasinya, pembagian data rahasia dapat dilakukan menjadi beberapa bagian yang banyak. Kemudian hanya beberapa bagian saja, sesuai aturan yang telah ditentukan sebelumnya, dapat direkonstruksikan nilai awal yang dicari.

Pada perkembangan selanjutnya, penggunaan skema pembagian rahasia ini telah mengalami perkembangan yang amat pesat salah satunya adalah skema pembagian rahasia menggunakan kode linear. Pada prinsipnya, setiap kode linear bisa digunakan untuk mengkontruksikan skema pembagian rahasia. Akan tetapi untuk menentukan struktur aksesnya

adalah hal yang sangat sulit. Hal ini dikarenakan memerlukan karakteristik yang lengkap dari codeword minimal yang berdasarkan pada kode linear.

Beberapa istilah yang sering dipakai dalam makalah ini antara lain partisipan, *share*, *secret*, himpunan akses minimal, serta struktur akses. *Secret* adalah informasi yang ingin dirahasiakan sedangkan partisipan merupakan anggota suatu himpunan yang diperbolehkan mengetahui *secret*. *Share* adalah bagian dari *secret* yang dibagikan kepada partisipan, sedangkan himpunan akses minimal adalah keluarga dari semua subhimpunan pertisipan yang dapat merekonstruksi *secret*.

Tulisan pada makalah ini secara keseluruhan merupakan uraian detail dari paper yang ditulis oleh Ozaman dkk (2007). Untuk dasar teori mengenai struktur aljabar, khususnya lapangan hingga dan ruang vektor atas lapangan hingga digunakan buku karangan Fraleigh (1982) dan buku karangan Mordeson-Malik (2000). Pembahasan yang berisi tentang definisi, teorema, dan proposisi tentang dasar-dasar pengkodean diambil dari buku yang ditulis oleh San Ling dan Chaoping Xing (2004) serta buku karangan Vanstone dan Oorschot (1989).

## PEMBAHASAN

Suatu lapangan hingga $F$ dengan banyak elemen $q$ dinotasikan dengan $F_q$. Lapangan $F_q$ dapat dipandang sebagai ruang vektor atas dirinya sendiri. Kemudian ruang vektor $F_q^n$ atas $F_q$ adalah himpunan semua vektor dengan panjang $n$ dengan entri-entri anggota $F_q$, atau

$$F_q^n = \{(v_1, v_2, \cdots, v_n): v_i \epsilon F_q\}$$

Selanjutnya kode linear $C$ dengan panjang $n$ atas lapangan hingga $F_q$ adalah *subspace* atau ruang (vektor) bagian dari ruang vektor $F_q^n$ (atas $F_q$). Elemen-elemen dalam $C$ disebut *codeword*. Pada ruang vektor terdapat beberapa operasi yaitu operasi antara vektor dengan skalar yang hasilnya vektor, ada pula operasi antar vektor yang hasilnya skalar. Selain itu ada operasi hasil kali dalam (*inner product*). Pada operasi hasil kali dalam ini dapat didefinisikan $C^\perp$, yaitu komplemen *orthogonal* dari $C$. Anggota-anggota dari $C^\perp$ adalah semua vektor tak nol yang hasil kali dalam dengan setiap anggota di $C$ adalah nol.

Prinsip dasar pengkodean adalah mendeteksi kesalahan (*error*) dalam pengiriman data dan memperbaikinya sehingga pesan yang dikirim dapat terbaca kembali. Proses ini disebut proses *encoding* dan *decoding*. Kemudian akan didefinisikan matriks pembangun dan matriks *parity-check* yang banyak digunakan dalam proses *encoding* dan *decoding.*

**Definisi 2.1.** Jika $C$ kode linear, maka:

a) *Matriks pembangun* untuk kode linear $C$ adalah matriks $G$ dimana baris-barisnya dibentuk dari basis $C$.
b) *Matriks parity-check H* untuk kode linear $C$ adalah matriks pembangun untuk kode dual $C^\perp$.

Ide awal dari skema pembagian rahasia menggunakan kode linear yaitu ketika *secret* dapat diubah atau diencode menjadi suatu *codeword* $(D_1, D_2, \dots, D_n)$. Andaikan diketahui jumlah $D_i$ dan menggunakan mekanisme *error correcting* dapat ditentukan $D_i$ sisanya dan dapat ditentukan *secret* utuhnya.

Diberikan kode linear $C \subset F_q^n$ dengan dimensi $k$ dan matriks pembangun $G = [g_{0,} g_1, \dots, g_{n-1}]$ dengan ukuran $k \times n$. Diasumsikan bahwa $G$ tidak memiliki kolom nol. *Secret* $s$ adalah elemen $F_q$, terdapat $n-1$ partisipan dan satu dealer. Untuk menentukan *share*, dealer memilih $t \in C$ yaitu $t = (t_0, \dots, t_{n-1})$ sedemikian sehingga $t_0 = s$. Kemudian dipilih $t$ dengan mengambil sebarang vektor $u = (u_0, \dots, u_{k-1}) \in F_q^k$ sedemikian sehingga $s = ug_0$. Akibatnya

$u$ dapat dipilih dengan $q^{k-1}$ cara. Sehingga $t$ dapat dihitung dengan $t = uG$, diperoleh *share*-nya adalah $\{t_1, t_2, \dots, t_{n-1}\}$ dan $G$ diketahui oleh semua partisipan.

Jika $g_0, g_{i_1}, \dots, g_{i_m}$ bergantung linear maka *secret* dapat ditentukan dengan cara sebagai berikut. Perhatikan bahwa

$$g_0 = \sum_{j=1}^{m} x_j g_{i_j}$$

setelah $x_j$ ditemukan, *secret* dapat dihitung sebagai

$$t_0 = ug_0 = \sum_{j=1}^{m} x_j u g_{i_j} = \sum_{j=1}^{m} x_j t_{i_j}$$

Untuk menentukan $g_0, g_{i_1}, \dots, g_{i_m}$ yang bergantung linear, terlebih dahulu akan dibahas mengenai hal-hal yang terkait untuk memudahkan dalam menentukan *secret*. Diasumsikan hanya ada satu jalan untuk menentukan *secret* dari sebarang himpunan *share*. Didefinisikan pendukung suatu vektor.

**Definisi 2.2.** *Pendukung suatu vektor* $v \in F_q^n$ didefinisikan sebagai $\{0 \le i \le n-1 : v_i \neq 0\}$.

Selanjutnya diberikan definisi cover.

**Definisi 2.3.** Vektor $v_1 \in F_q^n$ dikatakan *melingkupi\mengkover* $v_2 \in F_q^n$ jika pendukung vektor $v_1$ berada atau termuat di $v_2$.

Kemudian didefinisikan vektor minimal.

**Definisi 2.4.** Vektor $v \neq 0$ disebut *minimal* jika hanya melingkupi perkalian skalar dari $v$.

Selanjutnya diberikan definisi *codeword* minimal.

**Definisi 2.5.** Suatu *codeword* yang komponen pertamanya 1 dan melingkupi perkalian skalar disebut *codeword minimal*.

Setiap *codeword* minimal adalah vektor minimal, akan tetapi tidak berlaku sebaliknya.

Untuk suatu *codeword* $v = (1, v_1, \dots, v_{n-1}) \in C^{\perp}$ dengan tidak semua $v_j = 0$, *secret* dapat dibentuk kembali sebagai

$$vt = t_0 + v_1 t_1 + \cdots + v_{n-1} t_{n-1} = 0$$

dengan $v \in C^{\perp}, t \in C$.

Kemudian diperoleh

$$t_0 = -(v_1 t_1 + \cdots + v_{n-1} t_{n-1})$$

dimana $t_1, \dots, t_{n-1}$ adalah *share*-nya. Lebih lanjut jika terdapat $w \in C^{\perp}$ sedemikian sehingga

$$w = (1,0, \dots,0, w_{l_1}, 0, \dots,0, w_{l_m}, 0, \dots,0)$$

dengan tidak semua $w_{l_j} = 0$ maka $t_0$ dapat diperoleh dari

$$wt = t_0 + w_{l_1} t_{l_1} + \cdots + w_{l_m} t_{l_m}$$

Hal ini kemudian mendasari pemikiran bahwa himpunan akses minimal dapat ditentukan dengan *codeword-codeword* dalam kode dual $C^{\perp}$ dimana entri pertamanya adalah 1 dan melingkupi perkalian skalar yang dinamakan dengan *codeword* minimal. Hal ini berarti bahwa struktur akses dari skema ini seluruhnya ditentukan oleh *codeword* minimal.

Selanjutnya akan dibahas mengenai korespondensi antara vektor kolom yang bergantung linear dari $G$ dengan *codeword* di $C^{\perp}$ dengan proposisi di bawah ini.

**Proposisi 2.6.** *Kolom-kolom $g_{i_1}, \dots, g_{i_m}$ dari $G$ bergantung linear jika dan hanya jika terdapat suatu codeword $c = (0, \dots, 0, c_{i_1}, 0, \dots, 0, c_{i_m}, 0, \dots, 0) \in C^{\perp}$.*

**Bukti.** Misalkan $g_{i_r s}$ merupakan komponen ke-$s$ dari vektor kolom $g_{i_r}$. Jika $g_{i_1}, g_{i_2}, \dots, g_{i_m}$ bergantung linear maka terdapat $c_{i_1}, \dots, c_{i_m}$ yang tidak semua nol, sehingga

$$c_{i_1} g_{i_1} + c_{i_2} g_{i_2} + \cdots + c_{i_m} g_{i_m} = 0$$

Kemudian,

$$c_{i_1} g_{i_1 s} + \cdots + c_{i_m} g_{i_m s} = 0, \qquad \forall s = 0, \dots, m-1$$

Ambil sebarang $v \in C$. Karena $v$ kombinasi linear dari vektor baris dari $G$ diperoleh,

$$v = \sum_{j=0}^{m-1} a_j \, (g_{1j}, \dots, g_{(m-1)j})$$

Untuk $c = (0, \dots, 0, c_{i1}, 0, \dots, 0, c_{im}, 0, \dots, 0)$ diperoleh

$$\begin{aligned} vc &= \sum_{j=0}^{m-1} a_j \left(g_{1j}, \dots, g_{(m-1)j}\right)(0, \dots, 0, c_{i1}, 0, \dots, 0, c_{im}, 0, \dots, 0) \\ &= \sum_{j=0}^{m-1} a_j \left(c_{i_1} g_{i_1 j} + \cdots + c_{i_m} g_{i_1 j}\right) \\ &= \sum_{j=0}^{m-1} a_j \, 0 = 0 \end{aligned}$$

Sehingga, $c \in C^{\perp}$.

Sebaliknya, diketahui bahwa $c = (0, \dots, 0, c_{i1}, 0, \dots, 0, c_{im}, 0, \dots, 0) \neq 0 \in C^{\perp}$. Ambil sebarang $v \in C$, $v$ merupakan kombinasi linear dari vektor baris dari $G$, diperoleh

$$v = \sum_{j=0}^{m-1} a_j \, (g_{1j}, \dots, g_{(m-1)j})$$

Sehingga,

$$\begin{aligned} & vc = 0 \\ \Leftrightarrow & \sum_{j=0}^{m-1} a_j \left(g_{1j}, \dots, g_{(m-1)j}\right)(0, \dots, 0, c_{i1}, 0, \dots, 0, c_{im}, 0, \dots, 0) = 0 \\ \Leftrightarrow & \sum_{j=0}^{m-1} a_j \left(c_{i_1} g_{i_1 j} + \cdots + c_{i_m} g_{i_1 j}\right) = 0 \end{aligned}$$

Karena $a_j \neq 0$ maka $c_{i_1} g_{i_{1j}} + \cdots + c_{i_m} g_{i_{1j}} = 0$. Sehingga, tidak semua $c_{i_1}, \ldots, c_{i_m} \neq 0$. Dengan kata lain, vektor-vektor $g_{i_1}, \ldots, g_{i_m}$ bergantung linear. ■

**Proposisi 2.7.** *Misalkan $c_1$ dan $c_2$ adalah codeword minimal yang berbeda di $C$ maka $c_1$ dan $c_2$ tidak nol pada komponen yang sama.*

**Bukti.** Andaikan pada komponen yang sama pada *codeword* $c_1$ dan $c_2$ adalah 0. Karena $c_1$ dan $c_2$ merupakan *codeword* yang berbeda terdapat suatu komponen ke-$j$ yang berbeda. Misalkan $c_1 = (1, \ldots, a, \ldots)$ dan $c_2 = (1, \ldots, b, \ldots)$ dimana $a$ dan $b$ komponen ke-$j$, $a \neq b, a \neq 0, b \neq 0$ maka $c_3 = c_2 - a^{-1}bc_1$ juga merupakan *codeword* di $C$. Perhatikan bahwa pendukung vektor $c_3$ merupakan subset sejati dari pendukung vektor $c_1$ dan $c_2$. Diperhatikan juga bahwa komponen pertama dari $c_3$ adalah tak nol. Sehingga, $c_4 = (1 - a^{-1}b)c_3$ merupakan *codeword* dengan komponen pertama adalah 1 dan bukan merupakan pergandaan skalar dari $c_1$ dan $c_2$ serta $c_1$ dan $c_2$ menutupi $c_4$. Kontradiksi dengan yang diketahui yaitu $c_1$ dan $c_2$ merupakan *codeword* minimal. Jadi, $c_1$ dan $c_2$ tak nol pada komponen yang sama. ■

Sebarang himpunan dari partisipan yang termasuk dalam himpunan akses akan dapat merekonstruksi *secret*. Akan tetapi kita hanya tertarik pada himpunan dari partisipan yang dimana sebarang subsetnya tidak dapat merekonstruksi *secret*. Kemudian diberikan definisi mengenai himpunan akses minimal.

**Definisi 2.8.** Suatu himpunan dari partisipan disebut *himpunan akses minimal* jika himpunan ini dapat menentukan kembali *secret* awal dengan mengkombinasikan *share* yang mereka miliki tetapi sebarang subset dari himpunan ini tidak bisa menentukan *secret*.

**Definisi 2.9.** *Struktur akses* dari suatu skema pembagi rahasia adalah himpunan dari semua himpunan akses minimal.

Pada beberapa kasus, terdapat suatu partisipan yang berada di semua himpunan akses minimal, sehingga untuk menentukan *secret* tidak mungkin tanpa partisipan ini. Partisipan yang seperti ini disebut partisipan diktator. Kemudian suatu skema pembagi rahasia disebut demokratis berderajat $t$ jika setiap grup dari $t$ partisipan berjumlah sama dengan himpunan akses minimal.

Sebelum menentukan korespondensi antara *codeword* minimal dengan himpunan akses

minimal, terlebih dahulu akan dijelaskan mengenai beberapa hal yang terkait.

**Proposisi 2.10.** *Jika* $\{P_{i_1}, \dots, P_{i_m}\}$ *adalah himpunan akses minimal maka kolom-kolom yang berkorespondensi* $g_{i_1}, \dots, g_{i_m}$ *bebas linear.*

**Bukti.** Untuk suatu himpunan akses minimal $\{P_{i_1}, \dots, P_{i_m}\}$ andaikan bahwa $g_{i_1}, \dots, g_{i_m}$ bergantung linear, maka

$$\lambda_1 g_{i_1} + \cdots + \lambda_m g_{i_m} = 0 \qquad (2.1.1)$$

dimana tidak semua $\lambda_j = 0$. Tanpa mengurangi keumuman, diasumsikan $\lambda_1 = 0$. Sehingga, $g_{i_1}$ dapat ditentukan dengan menyelesaikan persamaan linear (2.1.1). Sehingga partisipan $\{P_{i_2}, \dots, P_{i_m}\}$ dapat mengetahui *share* yang dimiliki oleh $P_{i_1}$ dengan mengkombinasikan *share* yang mereka miliki. Oleh karena itu, partisipan $\{P_{i_2}, \dots, P_{i_m}\}$ dapat merekonstruksi *secret* awal. Kontradiksi dengan $\{P_{i_1}, \dots, P_{i_m}\}$ merupakan himpunan akses minimal. Jadi, $g_{i_1}, \dots, g_{i_m}$ bebas linear. ■

Selanjutnya akan dijelaskan mengenai korespondensi antara *codeword* minimal dan himpunan akses minimal.

**Proposisi 2.11.** *Terdapat korespondensi satu-satu antara codeword minimal dan himpunan akses minimal dengan arti bahwa untuk setiap himpunan akses minimal* $\{P_{i_1}, \dots, P_{i_m}\}$ *terdapat suatu codeword minimal yang unik,*

$$c = (1,0, \dots,0, c_{i_1}, 0, \dots,0, c_{i_m}, 0, \dots,0) \in C^{\perp}$$

*sedemikian sehingga* $c_{ij} \neq 0$ *untuk suatu* $j = 1, \dots, m$ *dan begitu juga sebaliknya.*

**Bukti.** Jika $\{P_{i_1}, \dots, P_{i_m}\}$ merupakan himpunan akses minimal maka kolom-kolom $g_0, g_{i_1}, \dots, g_{i_m}$ bergantung linear. Dari Proposisi 2.6, terdapat

$$a = (a_0, 0, \cdots,0, a_{i_1}, 0, \cdots,0, a_{i_m}, 0, \cdots,0) \in C^{\perp}$$

dengan $a_0 \neq 0$ jika tidak

$$(0,0, \cdots,0, a_{i_1}, 0, \cdots,0, a_{i_m}, 0, \cdots,0) \in C^{\perp}$$

yang merupakan kontradiksi dengan Proposisi 2.6 dan 2.10. Diberikan

$$c = a_0^{-1} a = (1,0, \cdots,0, c_{i_1}, 0, \cdots,0, c_{i_m}, 0, \cdots,0)$$

Jika $c_{i_j} = 0$ untuk suatu $j \in \{1, \cdots, m\}$ maka berdasarkan Proposisi 2.10 bahwa $\{P_{i_1}, \cdots, P_{i_{j-1}}, P_{i_{j+1}}, \cdots, P_{i_m}\}$ dapat merekonstruksi *secret*. Hal ini kontradiksi dengan $\{P_{i_1}, \dots, P_{i_m}\}$ merupakan himpunan akses minimal.

Jika $c$ bukan vektor minimal maka $c$ melingkupi suatu vektor $\overline{c} \neq 0$ dan $c \neq \lambda \overline{c}$ untuk sebarang skalar $\lambda$. Dengan Proposisi 2.10, $\overline{c_0} \neq 0$. Misalkan $\overline{\overline{c}} = \bar{c} c_0 - \bar{c} \neq 0$, $c$ melingkupi $\bar{\bar{c}}$ dan $\overline{\overline{c_0}} = 0$. Jadi, $\bar{\bar{c}}$ memiliki bentuk

$$(0,0, \cdots,0, \overline{\overline{c_{i_1}}}, 0, \cdots,0, \overline{\overline{c_{i_m}}}, 0, \cdots,0) \in C^{\perp}$$

Hal ini kontradiksi dengan Proposisi 2.6 dan 2.10 dan oleh sebab itu $c$ merupakan *codeword* minimal. Ketunggalan *codeword* $c$ sudah terbukti dari Proposisi 2.6.

Selanjutnya akan dibuktikan pernyataan sebaliknya. Jika $c = (1,0,\cdots,0,c_{i_1},0,\cdots,0,c_{i_m},0,\cdots,0)$ merupakan *codeword* minimal maka $g_0, g_{i_1},\cdots,g_{i_m}$ bergantung linear berdasarkan Proposisi 2.6. Sehingga himpunan dari partisispan $\{P_{i_1},\dots,P_{i_m}\}$ dapat merekonstruksi *secret*. Jika sebarang subset sejati dari partisipan ini dapat merekonstruksi *secret* maka $\left\{P_{i_1},\cdots,P_{i_{j-1}},P_{i_{j+1}},\cdots,P_{i_m}\right\}$ juga dapat merekonstruksi *secret*. Hal ini mengakibatkan keterjaminan eksistensi dari suatu *codeword* tak nol yang melingkupi $c$. Kontradiksi dengan minimalitas $c$. Sehingga $\left\{P_{i_1},\dots,P_{i_m}\right\}$ merupakan himpunan akses minimal. ■

**Contoh 2.12.** Misalkan $C$ kode linear di $F_3^5$ dan ada 4 partisipan yang dinotasikan dengan $P_1, P_2, P_3, P_4$. Diberikan matriks *parity-check* dari $C$ yaitu,

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 2 \end{bmatrix}$$

Sehingga $H$ merupakan matriks pembangun dari $C^{\perp}$. Matriks pembangun untuk $C$ adalah

$$G = \begin{bmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} = [g_0 \quad g_1 \quad g_2 \quad g_3 \quad g_4]$$

Andaikan *secret* yang ingin dibagi adalah 2. Ambil sebarang *codeword* $t$ dari $C$ dimana komponen pertamanya adalah 2. Katakan $t = (22021)$ sehingga *share* yang dibagikan adalah $K_1 = 2,\ K_2 = 0, K_3 = 2, K_4 = 1$, dimana $K_i$ merupakan *share* dari $P_i$.

$C^{\perp} =$

$\{(11121),(00000),(10112),(20221),(22212),(02021),(01012),(12100),(21200)\}$.

Vektor minimal dari $C^{\perp}$ adalah $(10112),(20221),(02021),(01012),(12100),(21200)$. Sedangkan *codeword* minimalnya (10112) dan (12100). *Codeword* pertama menyatakan bahwa kolom-kolom $g_0, g_1, g_2$ bergantung linear dan sebarang subsetnya bebas linear sehingga $\{P_2, P_3, P_4\}$ merupakan himpunan akses minimal. Sedangkan *codeword* kedua menyatakan bahwa $\{P_1, P_2\}$ merupakan himpunan akses minimal yang lain. Sehingga $P_2$ berada di setiap himpunan akses minimal. Jadi $P_2$ merupakan partisipan diktator.

Himpunan $\{P_2, P_3, P_4\}$ dapat membentuk kembali *secret* awal dengan menyelesaikan sistem persamaan yang ditentukan, yaitu

$$g_0 = a_2 g_2 + a_3 g_3 + a_4 g_4$$

$$\Leftrightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = a_2 \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} + a_3 \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} + a_4 \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix}1\\0\\0\end{bmatrix} = \begin{bmatrix}2a_2\\a_2+a_4\\a_3+a_4\end{bmatrix}$$

Diperoleh solusi dari sistem persamaan di atas adalah $a_2 = 2$, $a_3 = 2$, dan $a_4 = 1$. Dengan mengkombinasikan *share* diperoleh

$$a_2K_2 + a_3K_3 + a_4K_4 = 2.0 + 2.2 + 1.1 = 2$$

Andaikan $P_4$ tidak ada dan $P_2, P_3$ ingin mengkombinasikan *share* yang mereka miliki agar bisa menemukan *secret*. Mereka perlu mencari *codeword* dimana komponen kedua adalah 0 dan komponen ketiga adalah 2. Dengan catatan bahwa indeks dimulai dari 0. Ada 3 *codeword* di $C$ yang memenuhi yaitu, (00022), (11020), dan (22021). Komponen ke-0 dari tiap *codeword* tersebut berbeda. Akibatnya dengan mengkombinasikan *share* yang dimiliki oleh $P_2$ dan $P_3$ tidak akan memberikan informasi apapun mengenai *secret*.

## KESIMPULAN

Masalah skema pembagian rahasia dapat diselesaikan dengan menggunakan kode linear. Pada prinsipnya, setiap kode linear bisa digunakan untuk mengkonstruksikan skema pembagi rahasia. Akan tetapi untuk menentukan struktur aksesnya adalah hal yang tidak mudah. Hal ini dikarenakan memerlukan karakteristik yang lengkap dari *codeword* minimal yang berdasarkan pada kode linear. Pada perkembangan selanjutnya dapat diselidiki atau diteliti pemakaian jenis-jenis kelas kode linear yang sifatnya jauh lebih khusus dan istimewa serta dapat dikembangkan mengenai metode pencarian *codeword* minimalnya.

## DAFTAR PUSTAKA

Fraleigh, John B., 1982, *A First Course in Abstract Algebra,* Addison Wesley, USA.

Ling, San and Chaoping X., 2004, *Coding Theory, A First Course,* Cambridge University Press, USA.

Malik, D.S., 2000, *Fundamentals of Abstract Algebra,* Mc Graw Hill, USA.

Ozaman, Hakan, and F. Ozbudak, Z. Saygi., 2007, *Secret Sharing Schemes and Linear Codes,* ISC Turkey, Turkey.

Vanstone, S.A dan Scott A.O., 1989, *An Introduction to Error Correction with Aplications,* Kluwer Academic Publisher, USA.