UNIVERSITAS INDONESIA

ANALISIS PERBANDINGAN SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR AKSES DAN STRUKTUR TERLARANG BERDASARKAN GRAF

TESIS

RETNO INDAH
0806420234

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM MAGISTER MATEMATIKA
DEPOK
JULI 2010

UNIVERSITAS INDONESIA

ANALISIS PERBANDINGAN SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR AKSES DAN STRUKTUR TERLARANG BERDASARKAN GRAF

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Sains

RETNO INDAH
0806420234

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI MAGISTER MATEMATIKA
DEPOK
JULI 2010

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar

Nama	: Retno Indah
NPM	: 0806420234
Tanda Tangan	:
Tanggal	: 8 Juli 2010

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :
Nama : Retno Indah
NPM : 0806420234
Program Strudi : Magister Matematika
Judul Tesis : Analisis Perbandingan Skema Pembagian Rahasia Untuk Struktur Akses dan Struktur Terlarang Berdasarkan Graf

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelah Magister Sains pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing	: Dr. Kiki Ariyanti Sugeng	( )
Penguji	: Prof. Dr. Djati Kerami	( )
Penguji	: Dr. Sri Mardiyati, M.Kom	( )

Ditetapkan di : Depok
Tanggal : 8 Juli 2010

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat rahmat-Nya, Tesis ini dapat penulis selesaikan. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Master Sains Jurusan Matematika pada Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Indonesia.

Penulis menyadari bahwa penyusunan tesis ini tidak lepas dari bantuan dan bimbingan dari berbagai pihak, mulai dari masa perkuliahan sampai pada proses penyusunan. Oleh karena itu, penulis mengucapkan terima kasih kepada:

(1) Dr. Kiki Ariyanti Sugeng, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan Tesis ini;
(2) Bapak dan Ibu dosen pada Program Magister Matematika FMIPA UI yang tealah menuntun penulis sehingga bisa menyelesaikan Tesis ini;
(3) Lembaga Sandi Negara, institusi penulis yang telah memberikan kesempatan dan dukungan dalam perkuliahan dan penyelesaian Tesis ini;
(4) Orang tua dan keluarga besar penulis, yang telah memberikan dukungan moral, materiil serta doa yang tidak pernah berhenti;
(5) Suami tercinta, atas segala dukungan, semangat dan doanya;
(6) Teman seperjuangan angkatan 2008 yang selalu kompak dan telah membantu dalam segala hal;
(7) Rekan-rekan kerja pada Lembaga Sandi Negara atas segala bantuan dan dukungannya;
(8) Berbagai pihak yang tidak bisa disebutkan satu per satu yang telah membantu penyelesaian Tesis ini.

Akhir kata, penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tesis ini bermanfaat bagi pengembangan ilmu pengetahuan serta masyarakat luas.

Penulis

2010

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Retno Indah
NPM : 0806420234
Program Studi : Magister Matematika
Departemen : Matematika
Fakultas : Matematika dan Ilmu Pengetahuan Alam
Jenis Karya : Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia. Hak Bebas Biaya Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya berjudul:

Analisis Perbandingan Skema Pembagian Rahasia
Untuk Struktur Akses dan Struktur Terlarang Berdasarkan Graf

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Biaya Royalti Noneksklusif ini Universitas Indonesia berhak untuj menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 8 Juli 2010
Yang menyatakan:

(Retno Indah)

ABSTRAK

Nama : Retno Indah
Program Studi : Magister Matematika
Judul : Analisis Perbandingan Skema Pembagian Rahasia untuk Struktur Akses dan Struktur Terlarang Berdasarkan Graf

Keamanan data terhadap informasi rahasia (*secret*) smerupakan hal yang sangat penting, sehingga tidak setiap orang berhak mengakses informasi rahasia tersebut. Oleh karena itu diperlukan suatu metode yang dapat digunakan untuk mengatur siapa saja yang berhak mengakses rahasia tersebut. Salah satu metode yang dapat digunakan adalah skema pembagian rahasia. Skema pembagian rahasia adalah suatu metode untuk membagikan potongan-potongan rahasia kepada partisipan sedemikian sehingga hanya subhimpunan-subhimpunan dari himpunan partisipan yang memenuhi kualifikasi tertentu yang dapat merekonstruksi rahasia. Dalam skema pembagian rahasia terdapat skema yang berdasarkan Struktur Akses dan Struktur Terlarang. Struktur Akses adalah kumpulan dari subhimpunan-subhimpunan partisipan yang dapat merekonstruksi rahasia. Sedangkan Struktur Terlarang adalah kumpulan dari subhimpunan-subhimpunan partisipan yang tidak dapat merekonstruksi rahasia. Dalam tulisan ini dibandingkan dua jenis skema tersebut yang berbentuk graf, dilihat dari cara membangun *share* dan *information rate*nya. Berdasarkan graf yang digunakan, tahapan konstruksi pada skema dengan Struktur Akses lebih sederhana jika dibandingkan dengan skema dengan Struktur Terlarang. Berdasarkan konstruksi skema maka dapat disimpulkan kedua skema tersebut bukan skema yang saling komplemen meskipun representasi grafnya saling komplemen.

Kata Kunci :
Skema Pembagian Rahasia, Struktur Akses, Struktur Terlarang, *information rate.*

ABSTRACT

Nama : Retno Indah
Study Program : Magister of Mathematic
Title : Comparison Analysis of Secret Sharing Scheme for Access Structure and Prohibited Structure Based on Graphs

Data security of confidential information is something that is very important, so not everyone has access to such confidential information. Therefore we need a method that can be used to regulate anyone who has access the secret. One method that can be used is a secret sharing scheme. Secret sharing scheme is a method to distribute pieces of the secret to the participants such that only qualified subsets of the participants that can reconstruct the secret. In secret sharing schemes are schemes based on Access Structure and Prohibited Structure. Access Structure is a collection of subsets of participants that can reconstruct the secret. While the Prohibited Structure is a collection of subsets of participants who can not reconstruct the secret. In this paper we compare two types of such schemes based on graphs, and we see from the process of building the share and from the information rate. Based on the graph is used, the stages of construction on the scheme with access structure is simpler than the scheme with access structure. The two schemes are not complement to each other, even the graph representations are complement each other.

Key Words :
Secret Sharing Scheme, Access Structure, Prohibited Structure, *Information Rate.*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Skema pembagian rahasia merupakan salah satu metode penting dalam *data security*. Salah satunya adalah berkaitan dengan manajemen kunci yang akan digunakan untuk mengenkripsi suatu berita dan mendekripsi suatu berita sandi. Suatu berita sandi tidak akan bisa didekripsi jika kunci yang akan digunakan untuk mendekripsinya rusak atau hilang. Oleh karena itu, suatu kunci harus disimpan di dalam sebuah tempat yang aman atau diberikan kepada seseorang yang dapat dipercaya. Akan tetapi jika tempat penyimpanan kunci tersebut rusak, atau orang yang dipercaya tersebut meninggal dunia, maka berita sandi tersebut tidak dapat didekripsi kembali, khususnya jika kunci yang digunakan berbentuk One Time Pad (OTP). Masalah lain yang mungkin timbul adalah apabila pemegang kunci menyalahgunakan wewenang atau melakukan kecurangan.

Solusi yang mungkin untuk mengatasi masalah ini adalah dengan membuat duplikat kunci tersebut dan menyimpannya didalam beberapa tempat yang aman atau memberikannya kepada beberapa orang yang dapat dipercaya, sehingga hanya orang-orang yang memenuhi kualifikasi tertentu yang bisa mendapatkan kunci tersebut. Untuk mengatur siapa saja yang berhak mendapatkan kunci tersebut digunakan suatu metode yang dikenal dengan skema pembagian rahasia.

Skema pembagian rahasia adalah suatu metode untuk membagikan potongan-potongan suatu rahasia kepada beberapa pihak sedemikian sehingga hanya himpunan dari pihak-pihak yang memenuhi suatu syarat tertentu yang dapat merekonstruksi rahasia tersebut. Pada prinsipnya, skema pembagian rahasia digunakan pada segala hal yang apabila penanganannya diberikan hanya kepada satu orang saja, maka besar kemungkinan terjadi penyalahgunaan terhadap wewenang tersebut.

Suatu skema pembagian rahasia dikatakan sempurna atau *perfect secret Sharing Scheme* jika tidak mungkin bagi pihak-pihak yang tidak memenuhi persyaratan tertentu dapat merekonstruksi informasi tentang rahasia tersebut,

meskipun hanya sebagian informasi. Sedangkan suatu skema pembagian rahasia dikatakan tidak sempurna atau *nonperfect secret sharing scheme* jika terdapat pihak-pihak yang memiliki suatu bagian informasi tentang rahasia tetapi tidak dapat merekonstruksi rahasia tersebut secara lengkap.

Dalam skema pembagian rahasia terdapat konstruksi yang berdasarkan struktur akses dan berdasarkan struktur terlarang. Struktur akses adalah kumpulan dari subset-subset partisipan yang dapat merekonstruksi rahasia. Sedangkan struktur terlarang adalah kumpulan dari subset-subset partisipan yang tidak dapat merekonstruksi rahasia. Skema pembagian rahasia dapat dinyatakan antara lain dalam bentuk graf.

1.2 Perumusan Masalah

1.2.1 Masalah Umum

Bagaimana konstruksi skema pembagian rahasia untuk struktur akses yang direpresentasikan dalam graf?

1.2.2 Masalah Khusus

Masalah khusus yang akan dibahas pada skema pembagian rahasia dengan struktur berbentuk graf adalah perbandingan antara skema pembagian rahasia yang berdasarkan struktur akses Γ dengan skema pembagian rahasia berdasarkan struktur terlarang Δ.

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengkaji perbandingan antara skema pembagian rahasia *perfect* untuk struktur akses Γ dan struktur terlarang Δ berdasarkan graf dengan melihat:

a) Bagaimana unsur *share* dari masing-masing skema tersebut dibangun
b) *Information rate* dari konstruksi skema pembagian rahasia yang dikaji.

1.4 Manfaat Penelitian

Manfaat dari penelitian yang dilakukan adalah:

a) Diharapkan hasil penelitian ini dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan yang berkaitan dengan *secret sharing*, khususnya yang konsepnya berdasarkan graf.
b) Diharapkan hasil penelitian ini dapat diaplikasikan pada bidang lain yang memanfaatkan konsep skema pembagian rahasia.

1.5 Sistematika Penulisan

BAB 1 : PENDAHULUAN

Bab ini berisi latar belakang, perumusan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

BAB 2 : SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR AKSESBERDASARKAN GRAF

Bab ini berisi tentang skema pembagian rahasia, struktur akses, skema *(t,n) threshold*, *information rate* dan teori tentang graf.

BAB 3 : SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR AKSESBERDASARKAN GRAF

Bab ini berisi tentang skema pembagian rahasia dengan struktur akses berdasarkan graf , *information rate* dan contohnya.

BAB 4 : SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR TERLARANG BERDASARKAN GRAF

Bab ini berisi tentang skema pembagian rahasia dengan struktur terlarang berdasarkan graf , *information rate* dan contohnya.

BAB 5 : ANALISIS PERBANDINGAN SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR TERLARANG DAN STRUKTUR TERLARANG BERDASARKAN GRAF

Bab ini berisi tentang analisis perbandingan skema pembagian rahasia untuk struktur akses dan struktur terlarang berdasarkan graf dengan melihat persamaan dan perbedaannya.

BAB 6 : KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari penjelasan pada bab-bab sebelumnya dan saran.

BAB 2
LANDASAN TEORI

Pada bab ini akan diberikan beberapa landasan teori yang berkaitan dengan skema pembagian rahasia, mulai dari pengertian, ukuran *share,* struktur akses, skema *(t,n)-threshold*, *information rate* dan teori tentang graf.

2.1 Skema Pembagian Rahasia

2.1.1 Pengertian

Salah satu metode yang dapat digunakan untuk melindungi informasi rahasia adalah skema pembagian rahasia, dimana pada skema ini diatur sedemikian sehingga pihak-pihak yang tidak berkompeten tidak dapat mengakses informasi rahasia. Skema pembagian rahasia adalah suatu metode untuk membagikan potongan-potongan suatu rahasia kepada beberapa pihak sedemikian sehingga hanya himpunan dari pihak-pihak yang memenuhi kualifikasi tertentu saja yang dapat merekonstruksi rahasia tersebut (Ito et alm1987). Untuk lebih jelasnya dapat dilihat pada penjelasan berikut.

Misalkan terdapat $P = \{p_1, p_2, ..., p_n\}$ yang merupakan himpunan partisipan dan *K* adalah informasi rahasia atau juga sering disebut *master key*. Informasi rahasia *K* tersebut kemudian dipecah menjadi *n* bagian S_1, $S_2,\ldots,S_n$ yang disebut *share*, yang kemudian setiap *share* S_i diberikian kepada partisipan p_i , $i=1,\ldots,n,$ sedemikian sehingga:

- Jika $P' = \{p_{i_1}, p_{i_2}, ..., p_{i_j}\} \subset P$ adalah subhimpunan partisipan yang memenuhi kualifikasi, maka K dapat direkonstruksi dari $\{S_{i_1}, S_{i_2}, ..., S_{i_j}\}$.
- Jika $P' = \{p_{i_1}, p_{i_2}, ..., p_{i_j}\} \subset P$ adalah subhimpunan partisipan yang tidak memenuhi kualifikasi, maka K tidak dapat direkonstruksi dari $\{S_{i_1}, S_{i_2}, ..., S_{i_j}\}$.

Kumpulan subhimpunan dari partisipan yang dapat merekonstruksi kunci rahasia disebut struktur akses (Ito et al, 1987). Sedangkan kumpulan

subhimpunan dari partisipan yang tidak dapat merekonstruksi kunci rahasia disebut struktur terlarang (Jackson , 1994).

Berdasarkan sifatnya, skema pembagian rahasia dapat dibedakan menjadi skema pembagian rahasia *perfect* dan *nonperfect*. Suatu skema pembagian rahasia dikatakan *perfect* jika subhimpunan dari partisipan yang tidak mempunyai kualifikasi tidak bisa memperoleh informasi apapun tentang *K*. Sebaliknya apabila tidak memenuhi persyaratan tersebut, maka skema pembagian rahasia dikatakan *nonperfect*. Berdasarkan strukturnya, skema pembagian rahasia dapat direpresentasikan dalam bentuk graf maupun bentuk lain.

Skema pembagian rahasia pertama kali diperkenalkan oleh *A. Shamir* pada tahun 1979. Skema yang ditemukan Shamir dikenal dengan *(t,n)-threshold scheme* atau *Shamir's Secret Sharing Scheme* (Shamir, 1979). Secara terpisah, pada tahun yang sama *G. Blackley* juga menemukan skema pembagian rahasia.

2.1.2 Struktur Akses

Kumpulan dari semua subhimpunan partisipan P yang dapat merekonstruksi kunci rahasia disebut struktur akses, dinotasikan dengan Γ dimana $\Gamma \subset 2^P$ dan 2^P adalah himpunan dari semua subset P. Sedangkan kumpulan dari semua subhimpunan partisipan P yang tidak dapat merekonstruksi kunci rahasia disebut struktur terlarang, dinotasikan dengan Δ.

Misalkan $B \in \Gamma,$ dan $B \subseteq C \subseteq P$ maka $C \in \Gamma$. Jika Γ merupakan struktur akses, maka $B \in \Gamma$ disebut subhimpunan minimal dari Γ, jika $A \notin \Gamma$ dengan $A \subseteq B, A \neq B$. Kumpulan subhimpunan minimal dari Γ dinotasikan dengan Γ_0. Karena Γ terdiri dari semua subhimpunan P , yang merupakan superset dari subhimpunan dalam Γ_0, maka Γ dapat dinyatakan dengan $\Gamma = \{C \subseteq P : B \subseteq C, B \in \Gamma_0\}$ dan Γ_0 dapat disebut dengan stukrur akses minimal.

Berdasarkan struktur akses, skema pembagian rahasia diklasifikasikan menjadi tiga [Sun & Shieh, 1997), yaitu:

a) Tipe I: struktur akses Γ

   Skema pembagian rahasia untuk struktur akses Γ adalah sebuah metode membagikan *master key* kepada sejumlah berhingga partisipan dalam sebuah cara sedemikian sehingga hanya subhimpunan-subhimpunan dalam Γ yang dapat merekonstruksi *master key* K, sedangkan semua anggota $\Delta = 2^P \setminus \Gamma$ tidak dapat merekonstruksi K.

b) Tipe II: struktur terlarang Δ

   Skema pembagian rahasia untuk struktur terlarang Δ adalah sebuah metode membagikan *master key* kepada sejumlah berhingga partisipan dalam sebuah cara sedemikian sehingga hanya subhimpunan-subhimpunan dalam Δ yang tidak dapat merekonstruksi *master key* K, sedangkan semua anggota $\Gamma = 2^P \setminus \Delta$ dapat merekonstruksi K.

c) Tipe III: struktur campuran (Γ, Δ)

   Skema pembagian rahasia untuk struktur struktur campuran (Γ, Δ) adalah sebuah metode pembagian *master key* kepada sejumlah berhingga partisipan dalam sebuah cara sedemikian sehingga subhimpunan-subhimpunan dalam Γ dapat merekonstruksi *master key* K, tetapi subhimpunan-subhimpunan dalam Δ tidak dapat merekonstruksi *master key* K. Sub himpunan lain diluar dari Γ dan Δ yaitu $2^P \setminus (\Gamma \cup \Delta)$ tidak menjadi perhatian utama. Sembarang sub himpunan $2^P \setminus (\Gamma \cup \Delta)$ kemungkinan dapat merekonstruksi *master key K* tetapi bisa juga tidak dapat merekonstruksi *master key K*. Jadi $\Gamma \cap \Delta = \varnothing$ dan $\Gamma \cup \Delta \subset 2^P$.

Struktur akses Γ mempunyai sifat monoton naik, yaitu:

$$A \in \Gamma \text{ dan } A \subseteq B \subseteq P \Rightarrow B \in \Gamma$$

artinya jika suatu himpunan A mempunyai kualifikasi untuk merekonstruksi *master key*, yaitu $A \in \Gamma$, maka setiap superset dari A juga merupakan

suhimpunan yang memenuhi kualifikasi tersebut. Sedangkan struktur terlarang Δ mempunyai sifat monoton turun, yaitu:

$$A \in \Delta \text{ dan } B \subseteq A \subseteq P \Rightarrow B \in \Delta$$

artinya jika suatu himpunan A tidak mempunyai kualifikasi untuk merekonstruksi *master key*, yaitu $A \in \Delta$, maka setiap subhimpunan dari A juga tidak dapat merekonstruksi *master key*. [Stinson, 1992]

2.1.3 Skema *(t,n)-Threshold*

Skema *(t,n) threshold* pertama kali dikenalkan oleh Blakley dan Shamir pada tahun 1979 yang dikenal dengan skema *Shamir's (t,n)-threshold*. Ide utama yang mendasari skema (*t,n*)-*threshold* adalah membagi *master key* K menjadi n *share* S_i yang bersesuaian dengan partisipan P_i untuk *i=1,...,n*, dalam sebuah cara sedemikian sehingga *master key* tidak dapat diperoleh kembali kecuali jika *t share* dikumpulkan.

Skema (*t,n*)-*threshold* merupakan kasus khusus dari skema pembagian rahasia jika subhimpunan-subhimpunan partisipan yang dapat merekonstruksi *master key* (struktur akses Γ) adalah subhimpunan yang ordernya lebih besar atau sama dengan *t*, dan subhimpunan partisipan yang tidak dapat merekonstruksi *master key* (struktur terlarang Δ) adalah subhimpunan partisipan yang ordernya kurang dari atau sama dengan *t-1*. Atau dapat dinyatakan dengan:

$$\Gamma = \{A : |A| \geq t \text{ dan } A \subseteq P\}$$

Sedangkan struktur terlarangnya adalah:

$$\Delta = \{A : |A| < t \text{ dan } A \subseteq P\}$$

Konstruksi skema *Shamir's (t,n)-threshold* didasarkan pada interpolasi polinomial. Agar t-*share* dari *n* partisipan dapat merekonstruksi *master key* yang diberikan, maka dikonstruksi polinomial berderajat $(t-1)$ atas Z_q, dimana *q* adalah bilangan prima, dengan bentuk:

$$f(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}$$

sedemikian sehingga a_0 adalah informasi rahasia dan koefisien-koefisien yang lain adalah bilangan-bilangan acak dalam Z_q. Masing-masing *share* dari *n-share* tersebut (S_i) merupakan pasangan $(x_i, f(x_i))$ yang memenuhi $f(x_i) = y_i$ dan $x_i > 0$, dimana $i = 1,2,...,n$. Sehingga jika diberikan sembarang t *share*, maka polinomialnya dapat ditentukan dan informasi rahasia a_0 dapat dihitung menggunakan interpolasi Lagrange.

Sebagai contoh (Martana & Indah, 2010), misalkan diambil $K = 1234$ atas Z_{7789}. Informasi rahasia *K* ini akan didistribusikan menjadi 6 bagian, dimana 3 *share*-nya akan dapat digunakan untuk merekonstruksi *K*. Maka $n = 6$ dan $t = 3$. Karena $t = 3$, maka polinom yang akan dibuat berbentuk:

$$f(x) = a_0 + a_1 x + a_2 x^2$$

dengan $a_0 = K = 1234$.

Koefisien a_1 dan a_2 merupakan suatu bilangan yang dipilih secara acak dari Z_{7789}. Misalkan diambil $a_1 = 166$ dan $a_2 = 94$, maka polinom yang terbentuk adalah:

$$f(x) = 1234 + 166x + 94x^2$$

Dari polinom diatas, untuk $i = 1,2,...,6$ akan diperoleh:

$$S_1 = f(1) = 1494, \qquad S_4 = f(4) = 3402,$$
$$S_2 = f(2) = 1942, \qquad S_5 = f(5) = 4414,$$
$$S_3 = f(3) = 2578, \qquad S_6 = f(6) = 5614,$$

Nilai-nilai $S_i = (x_i, f(x_i))$ ini didistribusikan kepada partisipan ke-*i*, dimana *i=1,...,6*.

Untuk merekonstruksi *K* maka diperlukan 3 buah titik sembarang dari 6 nilai *share* S_i yang dimiliki. Misalkan 3 nilai yang digunakan adalah S_1,S_2, dan S_3, maka diperoleh:

$$(x_0, y_0) = (2,1942);$$
$$(x_1, y_1) = (4,3402);$$
$$(x_2, y_2) = (5,4414).$$

Untuk merekonstruksi polinom digunakan interpolasi Lagrange, yaitu:

$$l_k(x) = \prod_{\substack{i=0 \\ i \neq k}}^{k-1} \frac{x - x_i}{x_k - x_i}$$

$$l_0(x) = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5}$$
$$= \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$l_1(x) = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5}$$
$$= -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$l_2(x) = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4}$$
$$= \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

$$f(x) = \sum_{j=0}^{2} y_j \cdot l_j(x) \pmod{7789}$$

$$= 1942\left(\frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}\right) + 3402\left(-\frac{1}{2}x^2 + \frac{7}{2}x - 5\right)$$
$$+ 4414\left(\frac{1}{3}x^2 - 2x + \frac{8}{3}\right) \pmod{7789}$$

$$= \left(747 - 1942 + 1289\right)x^2 + \left(-3735 + 7768 - 3867\right)x$$
$$+ \left(4482 - 5826 + 2578\right) \pmod{7789}$$

$$= 94x^2 + 166x + 1234 \pmod{7789}$$

Sehingga diperoleh $K = a_0 = 1234$.

2.1.4 *Information Rate*

Karena keamanan dari sebuah sistem tergantung pada jumlah informasi yang harus diamankan, maka ukuran *share* yang diberikan kepada partisipan merupakan satu hal penting yang harus diperhatikan dalam mengkonstruksi suatu skema pembagian rahasia.

Tingkat efisiensi dari sebuah skema pembagian rahasia dapat dilihat dari *information rate*-nya, dimana *information rate* yang dinotasikan dengan

ρ adalah perbandingan antara ukuran *secret* dengan ukuran maksimum dari *share*.

Misalkan $P = \{p_1, p_2, ..., p_n\}$ adalah himpunan dari semua partisipan. Misalkan *K* adalah secret yang akan didistribusikan kepada himpunan partisipan *P*, sedangkan *share* dari partisipan ke-*i* ditunjukkan oleh S_i, untuk $i = 1, 2, ..., n$. Jika diterjemahkan dalam rangkaian biner, ukuran dari *K* adalah $\log_2|K|$, sedangkan ukuran dari *S* adalah $\log_2|S|$. Menurut Brickell dan Davenport (1991), *information rate* dari skema pembagian rahasia dinyatakan dengan:

$$\rho = \frac{\log_2|K|}{\max_i \log_2|S_i|}$$

Menurut (Karnin et al.,1992) dan (Capocelli et al., 1993), ukuran *share* dari setiap skema pembagian rahasia *perfect* lebih besar atau sama dengan ukuran informasi rahasianya., maka skema pembagian rahasia *perfect* akan memenuhi:

$$\log_2|S_i| \geq \log_2|K|$$

Sehingga *information rate* dari skema pembagian rahasia yang *perfect* adalah $\rho \leq 1$ (Brickell & Stinson,1990).

Sedangkan untuk skema pembagian rahasia *nonperfect*, ukuran *share*-nya bisa lebih kecil dari ukuran *secret*-nya. Suatu skema pembagian rahasia dikatakan ideal jika:

$$\log_2|S_i| = \log_2|K|$$

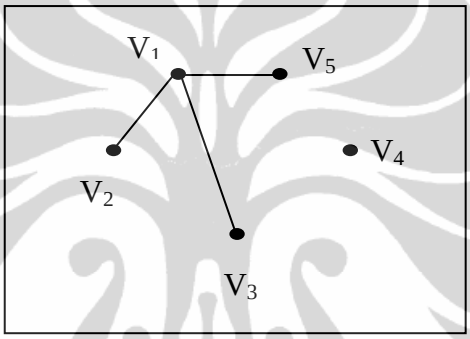
Sehingga *information rate* dari skema pembagian rahasia yang ideal adalah $\rho = 1$ (Brickell & Stinson,1990).

2.2 Graf

Graf merupakan suatu struktur diskrit yang terdiri atas simpul-simpul dan busur-busur yang menghubungkan simpul-simpul tersebut. [Rosen, 1999]. Berikut ini akan diberikan beberapa istilah yang berkaitan dengan graf.

Graf sederhana $G=(V,E)$ adalah sebuah graf yang terdiri dari V yang merupakan himpunan tak kosong dari simpul-simpul, dan E yang merupakan himpunan tak berurut pasangan elemen-elemen yang berbeda dari V yang disebut busur.

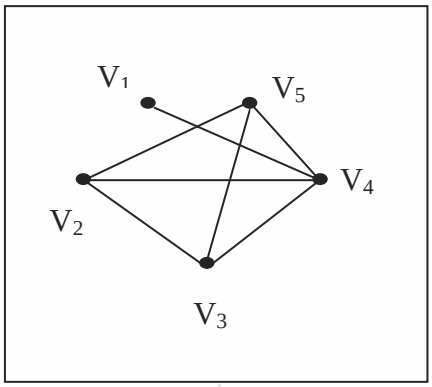
Graf sederhana juga merupakan sebuah graf yang tidak berarah yang tidak memiliki busur ganda maupun *loop*. Busur ganda merupakan busur-busur berbeda yang menghubungkan dua buah simpul yang sama. Sedangkan *loop* adalah sebuah busur yang menghubungkan sebuah simpul dengan dirinya sendiri. Pada Gambar 2.1 diperlihatkan contoh graf sederhana.



Gambar 2.1 Contoh graf sederhana G

Jika G adalah sebuah graf sederhana dengan himpunan simpul V(G), komplemen dari graf G yag dinotasikan dengan $\bar{G}$, adalah sebuah graf sederhana dengan himpunan simpul V(G) dimana dua buah simpulnya bertetangga jika dan hanya jika simpul-simpul tersebut tidak bertetangga di G. [Wilson, 1996]

Sebagai contoh, komplemen dari graf pada Gambar 2.1 adalah graf pada Gambar 2.2 .



Gambar 2.2 Komplemen dari graf gambar 2.1

Dua buah simpul u dan v dalam sebuah graf tak berarah G disebut bertetangga (*adjacent*) dalam G jika $\overline{uv}$ merupakan sebuah busur.[Wilson, 1996]. Jika $e = \overline{uv}$, busur e disebut *incident* dengan simpul u dan v. Busur e dikatakan menghubungkan u dan v. Simpul u dan v disebut titik ujung dari busur $\overline{uv}$.

Sebagai contoh, pada Gambar 2.2 simpul v_2 dan v_5 adalah dua simpul bertetangga.

Derajat dari sebuah simpul dalam suatu graf tak berarah adalah jumlah busur yang ber-*incident* dengan simpul tersebut. [Rosen, 1999]. Derajat dari simpul v dinotasikan dengan deg(v). Sebagai catatan sebuah *loop* memberikan dua kali derajat dari simpul tersebut

BAB 3
SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR AKSES BERDASARKAN GRAF

Sebuah skema pembagian rahasia memungkinkan sebuah *master key* dibagikan kepada himpunan partisipan dalam sebuah cara sedemikian sehingga hanya subhimpunan-subhimpunan tertentu dari partisipan tersebut yang dapat menemukan *master key*. Kumpulan dari subhimpunan partisipan yang dapat merekonstruksi *master key* disebut struktur akses dan dinotasikan dengan Γ. Struktur akses Γ bersifat monoton naik, yaitu jika $A \in \Gamma$ dan $A \subseteq B \subseteq P$, maka $\in \Gamma$. Γ. Kumpulan dari subhimpunan-subhimpunan partisipan yang tidak dapat merekonstruksi master key disebut struktur terlarang dan dinotasikan dengan Δ. Struktur Δ bersifat monoton turun yaitu jika $A \in \Delta$ dan $B \subseteq A \subseteq P$, maka $B \in \Delta$.

Pada sub bab berikut ini akan dijelaskan mengenai konstruksi skema pembagian rahasia untuk struktur akses berdasarkan graf beserta contohnya.

3.1 Konstruksi Skema pembagian rahasia Untuk Struktur Akses Berdasarkan Graf

Sebuah struktur akses pada skema pembagian rahasia berdasarkan graf adalah sebuah struktur akses yang ukuran dari tiap elemen dalam subhimpunan yang dapat merekonstruksi *master key* minimal sama dengan 2. Sebuah skema pembagian rahasia untuk struktur akses berdasarkan graf terdiri dari sebuah graf dimana sebuah simpul menotasikan seorang partisipan dan sebuah busur menotasikan minimal pasangan partisipan yang memenuhi kualifikasi. Sehingga jika dua partisipan dihubungkan oleh sebuah busur maka kedua partisipan tersebut dapat merekonstruksi *master key*.

Misalkan G adalah sebuah graf dengan himpunan simpul V(G), himpunan busur E(G) dan d adalah derajat maksimum dari graf G. Himpunan S adalah himpunan pasangan-pasangan partisipan yang bersesuaian dengan busur-busur dalam E(G). Misalkan $u, v \in V(G)$ dan $\overline{uv} \in E(G)$ maka $\{p_i, p_j\}$ dapat merekonstruksi *master key*, apabila partisipan p_i direpresentasikan

sebagai simpul u dan partisipan p_j direpresentasikan sebagai simpul v pada graf G.

Diasumsikan bahwa setiap partisipan yang bersesuaian dengan sebuah simpul dari G tidak dapat memperoleh informasi tentang *master key*. Hal ini dikarenakan jika seorang partisipan diperbolehkan untuk menyelesaikan *master key* dengan dirinya sendiri, maka hanya perlu memberikan *master key* sebagai *share*nya dan memindahkannya dari graf G. Graf tersebut dipandang mengandung graf yang tidak terhubung dan simpul terisolasi. Seorang partisipan yang bersesuaian dengan simpul terisolasi dapat diinterpretasikan bahwa dia tidak akan dapat menemukan *master key*.

Kumpulan dari subhimpunan partisipan yang dapat merekonstruksi *master key* disebut struktur akses dan dinotasikan dengan Γ dan dinyatakan dengan $\Gamma = \{B \subseteq P \,|\, B \supseteq A, A \in \Gamma_0\}$. Struktur akses Γ mempunyai sifat monoton naik, yaitu:

$A \in \Gamma$ dan $A \subseteq B \subseteq P \Rightarrow B \in \Gamma$

artinya jika suatu himpunan A dapat merekonstruksi *master key*, yaitu $A \in \Gamma$, maka setiap superset dari A juga dapat merekonstruksi *master key*.
Kumpulan subhimpunan minimal dari Γ dinotasikan dengan Γ_0 dinyatakan dengan $\Gamma_0 = \{B \in \Gamma : \exists A \notin \Gamma \text{ dengan } A \subseteq B, A \neq B\}$.

Kumpulan dari subhimpunan-subhimpunan partisipan yang tidak dapat merekonstruksi *master key* disebut struktur terlarang, dinotasikan dengan Δ dan dinyatakan dengan $\Delta = 2^P \setminus \Gamma = \{C \subseteq P \,|\, A \not\subset C, A \in \Gamma_0\}$. Struktur Terlarang Δ mempunyai sifat monoton turun, yaitu:

$A \in \Delta$ dan $B \subseteq A \subseteq P \Rightarrow B \in \Delta$

artinya jika suatu himpunan A tidak dapat merekonstruksi *master key*, yaitu $A \in \Delta$, maka setiap subhimpunan dari A juga tidak dapat merekonstruksi *master key*.
Berikut ini akan dijelaskan tentang konstruksi skema pembagian rahasia untuk struktur akses berdasarkan graf G.

Diasumsikan bahwa $P = \{p_1, p_2, ..., p_n\}$ adalah himpunan partisipan yang bersesuaian dengan simpul-simpul dari graf G. Untuk mengkonstruksi skema

pembagian rahasia dengan Struktur Akses maka dilakukan langkah-langkah berikut ini:

- **Langkah 1:**

  Tentukan q bilangan prima dan $q > n$. Tentukan *master key* K= (K_1,K_2) dimana K_1 dan K_2 diambil secara acak dari Z_q.

- **Langkah 2:**

  Tentukan fungsi polinomial atas Z_q sebagai berikut:

  $f(x) = K_2x + K_1$

- **Langkah 3:**

  Hitung nilai y_i dimana $y_i = f(i)$ untuk i=1,…,n

- **Langkah 4:**

  Pilih n bilangan acak atas Z_q, misalkan r_1, …, r_n,

- **Langkah 5:**

  Tentukan *share* dari masing-masing partisipan yang diberikan dengan:

  $S_i = \langle a_{i,1}, \dots, a_{i,t}, \dots, a_{i,n} \rangle$ dimana $1 \leq t \leq n$, dengan ketentuan

$$a_{i,t} = \begin{cases} r_i & \text{jika } t = i \\ r_t + y_t & \text{jika } t \neq i \text{ dan } \overline{p_i p_t} \in \mathrm{E(G)} \\ \text{kosong} & \text{jika } t \neq i \text{ dan } \overline{p_i p_t} \notin \mathrm{E(G)} \end{cases}$$

  Share S_i diberikan kepada partisipan p_i.

Pada langkah 2 fungsi polinomial yang digunakan adalah berderajat satu karena pada skema pembagian *master key* untuk Strktur Akses berdasarkan graf, banyaknya partisipan yang dibutuhkan untuk dapat merekonstruksi *master key* paling sedikit adalah dua. Hal ini sesuai dengan skema Shamir.

Berdasarkan langkah 2 dan langkah 3, jika sekelompok partisipan mempunyai y_i dan y_j untuk $i \neq j$, maka fungsi *f(x)* akan dapat ditentukan secara unik. Oleh karena itu jika sekelompok orang bisa memperoleh dua atau lebih y_i, maka kelompok tersebut akan dapat merekonstruksi *master key*. Tetapi jika sekelompok orang tidak mempunyai satupun nilai y_i maka kelompok tersebut tidak akan bisa merekonstruksi *master key*. Perlu dicatat bahwa seseorang yang mempunyai hanya satu bagian y_i maka orang tersebut akan mendapatkan sebagian informasi tentang *master key*.

Berdasarkan sifat-sifat dari konstruksi skema pembagian *master key* dengan Struktur Akses tersebut, maka konstruksi yang dibuat memenuhi sifat dalam teorema-teorema berikut. Teorema berikut dibuat dengan mengikuti ide dari (Wang & Juan, 2007).

Teorema 3.1.1

Jika $A \subseteq P$ dan $|A| < 2$ maka A tidak dapat merekonstruksi *master key* K.

Bukti:

Untuk $|A| = 0$, jelas bahwa tidak ada partisipan yang akan merekonstruksi *master key*, karena $A = \phi$.

Untuk $|A| = 1$ dan diasumsikan A=$\{p_i\}$ dimana $1 \leq i \leq n$. *Share* $S_i = \{a_{i,1}, ..., a_{i,t}, ..., a_{i,n}\}$ adalah *share* dari p_i. Jelas bahwa tidak ada informasi tentang y_i untuk semua $1 \leq i \leq n$. Sehingga partisipan p_i tidak dapat merekonstruksi *master key* K. □

Teorema 3.1.2

Misalkan $e = \overline{p_i p_j}$ untuk semua i dan j, $1 \leq i, j \leq n$, jika $\{p_i, p_j\} \not\subset A \subseteq P \forall e \in \Gamma_0$ dan $|A| \geq 2$ maka A tidak dapat merekonstruksi *master key* K.

Bukti:

Misalkan A=$\{p_i, p_j\}$, $1 \leq i < j \leq n$. *Share* dari p_i adalah $S_i = \{a_{i,1}, ..., a_{i,t}, ..., a_{i,n}\}$ dan *share* dari p_j adalah $S_j = \{a_{j,1}, ..., a_{j,t}, ..., a_{j,n}\}$ dimana $1 < t < n$. Karena $e \not\subset A \subseteq P \ \forall e \in \Gamma_0$, jelas bahwa p_i memiliki a_{ii}= r_i, a_{ij}= kosong dan p_j memiliki a_{jj}= r_j, a_{ji}= kosong. Maka p_i dan p_j tidak mempunyai informasi tentang y_i, sehingga *master key* K tidak dapat direkonstruksi. □

Teorema 3.1.3

Jika $\exists e \in E(G)$ dengan $e = \overline{p_i p_j}$ untuk suatu i dan j , $1 \le i,\ j \le n$ dan $\{p_i, p_j\}$ ada, $e \subseteq A \subseteq P$ dan $|A| \ge 2$, maka A dapat merekonstruksi *master key* K.

Bukti:

Misalkan $\{p_i,\ p_j\} \subseteq A$ untuk suatu $e = \overline{p_i p_j} \in \Gamma_0$ dimana $i \ne j$ dan Γ_0 bersesuaian dengan *S*. *Share* dari p_i adalah $S_i = \{a_{i,1}, ..., a_{i,t}, ..., a_{i,n}\}$ dan *share* dari p_j adalah $S_j = \{a_{j,1}, ..., a_{j,t}, ..., a_{j,n}\}$ dimana $1 < t < n$. Karena $\{p_i,\ p_j\} \in S$ maka $\overline{p_i p_j} \in E(G)$. Jadi p_i memiliki $a_{ii} = r_i$, $a_{ij} = r_j + y_j$ dan p_j memiliki $a_{jj} = r_j$, $a_{ji} = r_i + y_i$. Sehingga p_i dan p_j dapat merekonstruksi *master key* K. □

3.2 *Information rate*

Tingkat efisiensi dari sebuah skema pembagian rahasia dapat dilihat dari *information rate*nya, dimana *information rate* yang dinotasikan dengan ρ adalah perbandingan antara ukuran rahasia atau *master key* dengan ukuran maksimum dari *share*.

Information rate dari skema pembagian rahasia menurut [Brickell dan Davenport,1991] adalah :

$$\rho = \frac{\log_2 |K|}{\max_i \log_2 |S_i|}$$

dimana K adalah rahasia atau *master key* dan S_i adalah *share* dari partisipan ke-i. Dari rumus tersebut terlihat bahwa yang dijadikan dasar dalam penentuan *information rate*nya adalah ukuran rahasia dan ukuran *share*.

Selain berdasarkan ukuran *master key* dan ukuran *share*, penentuan *information rate* dapat juga dihitung berdasarkan graf yang digunakan. Salah satunya adalah perhitungan *information rate* berdasarkan [Sun,1999], yang dinyatakan dengan:

$$\rho = \frac{2}{d_{\max} + 1}$$

dimana $d_{\max}$ adalah derajat maksimum dari graf G. Hal ini dapat ditunjukkan sebagai berikut.

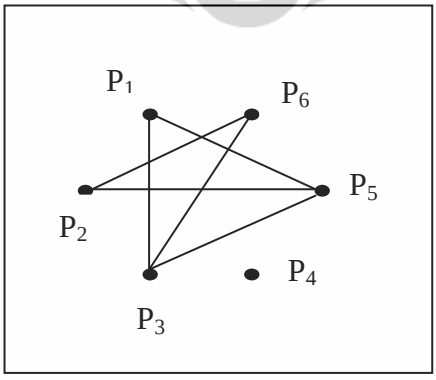
Share dari partisipan p_i adalah $S_i = \langle a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n} \rangle$. Kecuali jika nilai $a_{i,j}$ kosong (untuk semua j, $\overline{p_i p_j} \in E(G)$) setiap a_{ij} atas Z_q). Panjang dari *share* S_i adalah $\log(q^{d_i+1})$, dimana d_i adalah derajat simpul p_i di G. Panjang maksimal dari *share* adalah $\log(q^{d_{max}+1})$, dimana d_{max} adalah derajat maksimum dari graf G. Panjang *master key* adalah $\log(q^2)$. Sehingga *information rate* dari Skema pembagian rahasia untuk Struktur Akses ini adalah:

$$\rho = \frac{\log_2 |K|}{\max_i \log_2 |S_i|} = \frac{\log_2 (q^2)}{\log_2 (q^{d_{\max}+1})} = \frac{2 \log_2 2^r}{(d_{\max}+1) \log_2 2^r} = \frac{2}{d_{\max}+1}$$

dimana r merupakan panjang rangkaian biner dari masing-masing elemen K dan S_i.

3.3 Contoh Konstruksi Untuk Struktur Akses

Berikut ini akan diberikan contoh konstruksi skema pembagian rahasia untuk Struktur Akses dengan 6 partisipan yang dapat digambarkan dalam graf berikut.



Gambar 3.1 : Graf G

Berdasarkan Gambar 3.1, dapat dilihat bahwa:

$P = \{p_1, p_2, p_3, p_4, p_5, p_6, \}$

$E(G) = \{\overline{p_1p_3}, \overline{p_1p_5}, \overline{p_2p_5}, \overline{p_2p_6}, \overline{p_3p_5}, \overline{p_3p_6}\}$

$S = \{\{p_1,p_3\}, \{p_1, p_5\}, \{p_2,p_5\}, \{p_2,p_6\}, \{p_3,p_5\}, \{p_3,p_6\}\}$

Struktur Akses dari skema pembagian rahasia yang direpresentasikan pada Gambar 3.1 adalah:

$\Gamma_G = \{\{p_1,p_3\}, \{p_1, p_5\}, \{p_2,p_5\}, \{p_2,p_6\}, \{p_3,p_5\}, \{p_3,p_6\}, \{p_1, p_2, p_3\}, \{p_1, p_2, p_5\},$
$\{p_1, p_2, p_6\}, \{p_1, p_3, p_4\}, \{p_1, p_3, p_5\}, \{p_1, p_3, p_6\}, \{p_1, p_4, p_5\}, \{p_1, p_5, p_6\},$
$\{p_2, p_3, p_5\}, \{p_2, p_3, p_6\}, \{p_2, p_4, p_5\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_6\}, \{p_3, p_4, p_5\},$
$\{p_3, p_4, p_6\}, \{p_3, p_5, p_6\}, \{p_1, p_2, p_3, p_4\}, \{p_1, p_2, p_3, p_5\}, \{p_1, p_2, p_3, p_6\},$
$\{p_1, p_2, p_4, p_5\}, \{p_1, p_2, p_4, p_6\}, \{p_1, p_2, p_5, p_6\}, \{p_1, p_3, p_4, p_5\}, \{p_1, p_3, p_4, p_6\},$
$\{p_1, p_3, p_5, p_6\}, \{p_1, p_4, p_5, p_6\}, \{p_2, p_3, p_4, p_5\}, \{p_2, p_3, p_4, p_6\}\{p_2, p_3, p_5, p_6\},$
$\{p_2, p_4, p_5, p_6\}, \{p_3, p_4, p_5, p_6\}, \{p_1, p_2, p_4, p_5, p_6\}, \{p_1, p_3, p_4, p_5, p_6\},$
$\{p_2, p_3, p_4, p_5,p_6\}, \{p_1, p_2, p_3, p_4, p_5, p_6\}\}$

Sehingga Struktur Terlarang dari skema pembagian rahasia yang direpresentasikan pada Gambar 3.1 adalah:

$\Delta_G = \{\phi, \{p_1\}, \{p_2\}, \{p_3\}, \{p_4\}, \{p_5\}, \{p_6\}, \{p_1, p_2\}, \{p_1,p_4\}, \{p_1, p_6\},$
$\{p_2, p_3\}, \{p_2, p_4\}, \{p_3, p_4\}, \{p_4, p_5\}, \{p_4, p_6\}, \{p_5, p_6\}, \{p_1, p_2, p_4\},$
$\{p_1, p_4, p_6\}, \{p_2, p_3, p_4\}, \{p_4, p_5, p_6\}\}$

Tahap Konstruksi Skema pembagian rahasia adalah sebagai berikut:

- **Langkah 1:**

  Tentukan q = 163. Misalkan diambil *master key* K= (K_1,K_2) = (3,2) dimana K_1, K_2 diambil secara acak dari Z_{163}

- **Langkah 2:**

  Dibentuk fungsi polinomial f(x) dalam Z_{163} sebagai berikut:

  $f(x) = K_2x + K_1 = 2x + 3$

- **Langkah 3:**

  Hitung nilai y_i yang diperoleh dari f(x) dengan $y_i = f(i-1)$ untuk $i = 1, \dots, 6$.

Maka diperoleh

$$y_1 = f(1) = 2.1+3 = 5$$
$$y_2 = f(2) = 2.2+3 = 7$$
$$y_3 = f(3) = 2.3+3 = 9$$
$$y_4 = f(4) = 2.4+3 = 11$$
$$y_5 = f(5) = 2.5+3 = 13$$
$$y_6 = f(6) = 2.6+3 = 15$$

- **Langkah 4:**

  Pilih 6 bilangan acak atas Z_{163} misalkan

  $$r_1 = 2, r_2 = 3, r_3 = 5, r_4 = 7, r_5 = 11, r_6 = 13$$

- **Langkah 5:**

  Hitung *share* dari masing-masing partisipan dimana isi *share* dari p_i adalah

  $S_i = \langle a_{i,1}, \dots, a_{i,t}, \dots, a_{i,6} \rangle$ dimana $1 \leq t \leq 6$, dengan ketentuan:

  $$a_{i,t} = \begin{cases} r_i & \text{jika } t = i \\ r_t + y_t & \text{jika } t \neq i \text{ dan } \overline{p_i p_t} \in \mathrm{E(G)} \\ \text{kosong} & \text{jika } t \neq i \text{ dan } \overline{p_i p_t} \notin \mathrm{E(G)} \end{cases}$$

  Berdasarkan ketentuan di atas, *share* dari masing masing partisipan dapat dilihat pada Tabel 3.1 dan Tabel 3.2 berikut.

i	S_i	$a_{i,1}$	$a_{i,2}$	$a_{i,3}$	$a_{i,4}$	$a_{i,5}$	$a_{i,6}$
1	S_1	r_1	-	r_3+y_3	-	r_5+y_5	-
2	S_2	-	r_2	-	-	r_5+y_5	r_6+y_6
3	S_3	r_1+y_1	-	r_3	-	r_5+y_5	r_6+y_6
4	S_4	-	-	-	r_4	-	-
5	S_5	r_1+y_1	r_2+y_2	r_3+y_3	-	-	-
6	S_6	-	r_2+y_2	r_3+y_3	-	-	r_6

Tabel 3.1 Isi *share* dari masing-masing partisipan

i	S_i	$a_{i,1}$	$a_{i,2}$	$a_{i,3}$	$a_{i,4}$	$a_{i,5}$	$a_{i,6}$
1	S_1	2	-	14	-	24	-
2	S_2	-	3	-	-	24	28
3	S_3	7	-	5	-	24	28
4	S_4	-	-	-	7	-	-
5	S_5	7	10	14	-	11	-
6	S_6	-	10	14	-	-	13

Tabel 3.2 Nilai *share* dari masing-masing partisipan

Berikut ini akan diperlihatkan bahwa skema pembagian rahasia untuk Struktur Akses yang dibangun memenuhi:

a) Jika $A \subseteq P$ dan $|A| < 2$ maka A tidak dapat merekonstruksi *master key* K.

Untuk $|A| = 1$, misalkan jika diambil $A = \{p_1\}$.

Dari tabel 3.1 dan 3.2 diperoleh:

$$S_1 = \langle r_1, -, r_3 + y_3, -, r_5 + y_5, -, \rangle = \langle 2, -, 14, -, 24, -, \rangle$$

Dari S_1 terlihat bahwa p_1 tidak mempunyai informasi tentang y_i, sehingga A tidak dapat merekonstruksi *master key* K. Dengan cara yang sama dapat ditunjukkan bahwa sifat a) juga berlaku untuk p_i yang lain, untuk i=2,3,…,n.

b) Jika $e \not\subset A \subseteq P \ \forall e \in \Gamma_0$ dan $|A| \geq 2$ maka A tidak dapat merekonstruksi *master key* K.

- Untuk $|A| = 2$, misalkan jika diambil $A = \{p_1, p_2\}$.

  Dari tabel 1 dan 2 diperoleh:

$$S_1 = \langle r_1, -, r_3 + y_3, -, r_5 + y_5, -, \rangle = \langle 2, -, 14, -, 24, - \rangle$$

$$S_2 = \langle -, r_2, -, -, r_5 + y_5, r_6 + y_6 \rangle = \langle -, 3, -, -, 24, 28 \rangle$$

  Dari S_1 dan S_2 terlihat bahwa p_1 dan p_2 hanya memperoleh nilai r_1 dan r_2, sedangkan nilai y_i tidak diperoleh sama sekali, sehingga A tidak dapat merekonstruksi *master key* K.

- Untuk $|A| = 3$, misalkan jika diambil $A = \{p_2, p_{3,} p_4\}$.

  Dari tabel 3.1 dan 3.2 diperoleh:

  $$S_2 = \langle -, r_2, -, -, r_5 + y_5, r_6 + y_6 \rangle = \langle -,3, -, -,24,28 \rangle$$

  $$S_3 = \langle r_1 + y_1, -, r_3, -, r_5 + y_5, r_6 + y_6 \rangle = \langle 7, -, 5, -, 24, 28 \rangle$$

  $$S_4 = \langle -, -, -, r_4, -, - \rangle = \langle -, -, -,7, -, -, - \rangle$$

Dari S_2, S_3 dan S_4 terlihat bahwa p_2, p_3 dan p_4 hanya memperoleh nilai r_2, r_3 dan r_4, sedangkan nilai y_i tidak diperoleh sama sekali, sehingga A tidak dapat merekonstruksi *master key* K. Dengan cara yang sama dapat ditunjukkan bahwa sifat b) juga berlaku untuk pasangan partisipan lain yang tidak bersesuaian dengan busur di G

c) Jika $\exists e \in \Gamma_0, e \subseteq A \subseteq P$ dan $|A| \geq 2$ maka A dapat merekonstruksi *master key* K.

Untuk $|A| = 2$, misalkan jika diambil $A = \{p_1, p_3\} \epsilon \Gamma_0$.

Dari tabel 3.1 dan 3.2 diperoleh:

$$S_1 = \langle r_1, -, r_3 + y_3, -, r_5 + y_5, -, \rangle = \langle 2, -, 14, -,24, - \rangle$$

$$S_3 = \langle r_1 + y_1, -, r_3, -, r_5 + y_5, r_6 + y_6 \rangle = \langle 7, -, 5, -,24, 28 \rangle$$

Dari S_1 dan S_3, p_1 dan p_3 memperoleh nilai $r_1, r_3, r_1 + y_1, r_3 + y_3$ yang dapat digunakan untuk mencari nilai y_1 dan y_3, sehingga akan ditemukan *master key* K. Proses perhitungannya adalah sebagai berikut:

$r_1 = 2,\ r_1 + y_1 = 7$ maka $y_1 = 5$

$r_3 = 5,\ r_3 + y_3 = 14$ maka $y_3 = 9$

$y_1 = f(1) = K_2 . 1 + K_1 = 5$

$= \quad K_2 + K_1 = 5$ ……………………….……(1)

$y_3 = f(3) = K_2 . 3 + K_1 = 9$

$= \quad 3K_2 + K_1 = 9$ ………………………………(2)

Dari persamaan (1) dan (2) akan diperoleh $K_2 = 2$. Nilai $K_2 = 2$ kemudian disubstitusikan ke persamaan (1) hingga akhirnya diperoleh nilai $K_1 = 3$. Maka *master key* $K = (K_1, K_2) = (3,2)$ dapat direkonstruksi.

Dengan cara yang sama juga bisa dilakukan untuk pasangan partisipan lain yang bersesuaian dengan busur di G.

Berikut ini akan dihitung *information rate* dari contoh konstruksi skema pembagian rahasia yang dibuat.

- Berdasarkan Tabel 3.2 terlihat bahwa ukuran *share* S_i dari masing-masing partisipan dengan i=1,...,6 adalah: $|S_1| = 3, |S_2| = 3, |S_3| = 4, |S_4| = 1, |S_5| = 4, |S_6| = 3.$

  Ukuran dari *master key* adalah $|K| = 2$ .Maka berdasarkan berdasarkan [Brickell dan Davenport,1991] *information rate*nya adalah:

$$\rho = \frac{log_2|K|}{\max_i \log_2|S_i|} = \frac{log_2|2^8|^2}{log_2|2^8|^4} = \frac{2.log_2|2^8|}{4.log_2|2^8|} = \frac{1}{2}$$

- Dari Gambar 3.1 terihat bahwa derajat maksimum dari graf G adalah d_{max}=3. Maka berdasarkan [Sun, 1999], *information rate*nya adalah:

$$\rho = \frac{2}{d_{max}+1} = \frac{2}{3+1} = \frac{2}{4} = \frac{1}{2}$$

Dari hasil kedua perhitungan diatas, nilai *information rate* yang diperoleh adalah sama. Pada perhitungan *information rate* berdasarkan [Brickell dan Davenport, 1991], dimana untuk mencari ukuran maksimal dari *share*-nya harus melihat satu per satu dari masing-masing *share*, baru kemudian dihitung rasionya, sedangkan pada perhitungan berdasarkan [Sun, 1999] hanya cukup melihat dari struktur grafnya Sehingga dapat dikatakan bahwa proses perhitungan *information rate* berdasarkan Sun lebih sederhana jika dibandingkan berdasarkan [Brickell dan Davenport, 1991].

Pada bab berikutnya akan dibahas tentang skema pembagian rahasia untuk Struktur Terlarang berdasarkan graf.

BAB 4
SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR TERLARANG BERDASARKAN GRAF

Sebuah skema pembagian rahasia memungkinkan sebuah *master key* dibagikan kepada himpunan partisipan dalam sebuah cara sedemikian sehingga hanya subhim-punan-subhimpunan tertentu dari partisipan tersebut yang tidak dapat merekonstruksi *master key*. Misalkan P adalah himpunan partisipan. Kumpulan dari subhimpunan-subhimpunan partisipan yang dapat merekonstruksi *master key* disebut struktur akses dan dinotasikan dengan Γ. Kumpulan dari subhimpunan-subhimpunan partisipan yang tidak dapat merekonstruksi *master key* disebut struktur terlarang dan dinotasikan dengan Δ. Γ bersifat monoton naik dan Δ bersifat monoton turun yaitu:

jika $A \in \Gamma$ dan $A \subseteq B \subseteq P$, maka $B \in \Gamma$, dan
jika $A \in \Delta$ dan $B \subseteq A \subseteq P$, maka $B \in \Delta$.

4,1 Konstruksi Skema pembagian rahasia Untuk Struktur Terlarang Berdasarkan Graf

Dalam sebuah skema pembagian rahasia untuk Struktur Terlarang berdasarkan graf G, sepasang partisipan yang dihubungkan oleh sebuah busur dari G tidak dapat memperoleh bagian informasi dari *master key*. Hal ini berkebalikan dengan yang terjadi pada Struktur Akses. Diasumsikan juga bahwa setiap partisipan yang bersesuaian dengan sebuah simpul dari G tidak dapat memperoleh informasi tentang *master key*. Hal ini dikarenakan jika seorang partisipan diperbolehkan untuk menyelesaikan *master key* dengan dirinya sendiri, maka hanya perlu memberikan *master key* sebagai *share*nya dan memindahkan-nya dari graf G. Graf tersebut dipandang mengandung graf yang tidak terhubung dan simpul terisolasi. Seorang partisipan yang bersesuaian dengan simpul terisolasi dapat diinterpretasikan bahwa dia dapat menemukan *master key* bersama-sama dengan partisipan lain dalam graf tersebut kecuali dirinya sendiri.

Misalkan P adalah himpunan partisipan dan G adalah sebuah graf dimana sebuah simpul menotasikan seorang partisipan dalam P dan sebuah busur menotasikan pasangan partisipan. E (G) menotasikan himpunan busur dari G;

$E(\overline{G})$ menotasikan himpunan busur dari $\overline{G}$, dimana $\overline{G}$ adalah komplemen dari G. Himpunan S merupakan himpunan pasangan-pasangan partisipan yang bersesuaian dengan busur-busur dalam E(G). Himpunan R menyatakan himpunan pasangan-pasangan partisipan yang bersesuaian dengan busur-busur dalam $E(\overline{G})$. Kumpulan dari subhimpunan partisipan yang tidak dapat merekonstruksi *master key* disebut struktur terlarang, dinotasikan dengan Δ dan dinyatakan dengan

$$\Delta = \{A | A \subseteq P \text{ dan } |A| = 1\} \cup \{A | A \in S\}$$

Struktur Terlarang Δ mempunyai sifat monoton turun, yaitu:

$$A \in \Delta \text{ dan } B \subseteq A \subseteq P \Rightarrow B \in \Delta$$

artinya jika suatu himpunan A tidak dapat merekonstruksi *master key*, yaitu $A \in \Delta$, maka setiap subhimpunan dari A juga tidak dapat merekonstruksi *master key*.

Kumpulan dari subhimpunan partisipan yang dapat merekonstruksi *master key* disebut struktur akses, dinotasikan dengan Γ dan dinyatakan dengan

$$\Gamma = 2^P \setminus \Delta = \{A | A \subseteq P \text{ dan } |A| \geq 3\} \cup \{A | A \in R\}.$$

Struktur akses Γ mempunyai sifat monoton naik, yaitu:

$$A \in \Gamma \text{ dan } A \subseteq B \subseteq P \Rightarrow B \in \Gamma$$

artinya jika suatu himpunan A dapat merekonstruksi *master key*, yaitu $A \in \Gamma$, maka setiap superset dari A juga dapat merekonstruksi *master key*

Diasumsikan bahwa $P = \{p_1, p_2, ..., p_n\}$ adalah himpunan partisipan yang bersesuaian dengan simpul-simpul dari graf G. Untuk mengkonstruksi skema pembagian rahasia Struktur Terlarang maka dilakukan langkah-langkah berikut ini:

- **Langkah 1:**

  Tentukan *q* bilangan prima dengan *q* > *n*+2. Tentukan *master key* K= (K_1,K_2) dimana K_1,K_2 diambil secara acak dari Z_q.

- **Langkah 2:**

  Tentukan fungsi polinomial atas Z_q sebagai berikut:

  $$f(x) = K_2 x + K_1$$

- **Langkah 3:**

  Hitung nilai y_i dimana $y_i = f(i)$ untuk i=1,…,n+2.

- **Langkah 4:**

  Konstruksi dua buah skema (3,n)-*threshold* dengan nama TS_1 dan TS_2, untuk memproteksi y_{n+1} dan y_{n+2}. *Master key* dan *share* dari masing-masing TS_i disebut sub-*master key* dan sub-*share*.

  Untuk setiap (3,n)-TS_i, maka Sk_i adalah sub*master key*nya dimana $Sk_1 = y_{n+1}$ dan $Sk_2 = y_{n+2}$ sedangkan $s_{i,1}, s_{i,2},\ldots,s_{i,n}$ adalah n sub*share*nya .

- **Langkah 5:**

  Pilih n bilangan acak atas Z_q, misalkan $r_1, \ldots, r_n$,

- **Langkah 6:**

  Tentukan *share* dari masing-masing partisipan yang diberikan dengan:

  $S_i = \langle a_{i,1},...,a_{i,t},...,a_{i,n}, a_{i,n+1}, a_{i,n+2} \rangle$, dimana $1 \le t \le n$,

  $$a_{i,t} = \begin{cases} r_i & \text{, jika } t = i \\ r_i + y_i & \text{, jika } t \neq i \ \overline{p_i p_t} \in E(\bar{G}) \\ \text{kosong} & \text{, untuk yang lain} \end{cases}$$

  $$a_{i,n+2} = \begin{cases} s_{1,i} & \text{, } p_i \in T \\ \text{kosong} & \text{, untuk yang lain} \end{cases}$$

  $$a_{i,n+2} = \begin{cases} s_{2,i} & \text{, } p_i \in T \\ \text{kosong} & \text{, untuk yang lain} \end{cases}$$

  dimana T adalah himpunan partisipan ke-i dimana terdapat 2 partisipan lain sedemikian sehingga kombinasi 2 dari 3 partisipan tersebut membentuk sebuah busur. Jadi T dapat dinyatakan dengan

  $$T = \left\{ p_i \middle| \exists p_j \text{ dan } p_k \ \ni \ \overline{p_i p_j}, \overline{p_i p_k} \text{ dan } \overline{p_j p_k} \in E(G), i \neq j \neq k \right\}.$$

Pada langkah 2 fungsi polinomial yang digunakan adalah berderajat satu karena pada skema pembagian rahasia untuk Strktur Terlarang yang berdasarkan graf, banyaknya partisipan yang dibutuhkan untuk dapat merekonstruksi rahasia paling sedikit adalah dua. Hal ini sesuai dengan skema Shamir.

Jika seseorang mengetahui dua atau lebih y_i, $1 \le i \le n$, maka orang tersebut akan dapat merekonstruksi *master key* K. Tetapi jika seseorang tidak mengetahui nilai y_i maka orang tersebut tidak dapat memperoleh informasi tentang *master key*. Jika seseorang yang hanya mempunyai satu nilai y_i maka orang tersebut akan bisa memperoleh sebagian informasi tentang *master key*.

Berdasarkan langkah pada pembentukan (3,n)-TS_i, yang digunakan untuk memproteksi Sk_i, maka jika diberikan tiga sub*share* sembarang, $s_{i,j}$, $s_{i,k}$, $s_{i,l}$ $(1 \le j < k < l \le n)$, sub*master key* Sk_i dapat ditemukan, tetapi jika kurang dari tiga maka tidak akan diperoleh informasi tentang Sk_i.

Teorema 4.1.1 (Sun dan Shieh, 1999)

Jika $A \subseteq P$ dan $|A| > 2$, maka A tidak memperoleh informasi tentang *master key* dari konstruksi skema pembagian rahasia untuk Struktur Terlarang berdasarkan graf G.

Bukti:

Untuk $|A| = 0$, jelas bahwa tidak ada partisipan yang akan merekonstruksi *master key*, karena $A = \phi$.

Untuk $|A| = 1$, misalkan diasumsikan bahwa $A=\{p_i\}$ dan *share* dari p_i adalah $S_i = \langle a_{i,1}, ..., a_{i,t}, ..., a_{i,n}, a_{i,n+1}, a_{i,n+2} \rangle$. Ini jelas bahwa tidak ada informasi tentang y_j, $1 \le j \le n+2$, yang dapat diturunkan dari S_i karena di dalam S_i tidak terdapat nilai y_i yang berdiri sendiri. □

Teorema 4.1.2 [Sun dan Shieh, 1999]

Jika $A \in S$, maka A tidak memperoleh informasi tentang *master key* dari konstruksi skema pembagian rahasia untuk Struktur Terlarang berdasarkan graf G.

Bukti:

Diasumsikan bahwa $A = \{p_i, p_j\}$, dimana $i \neq j$. *Share* dari p_i adalah $S_i = \langle a_{i,1}, ..., a_{i,t}, ..., a_{i,n}, a_{i,n+1}, a_{i,n+2} \rangle$ dan share dari p_j adalah $S_j = \langle a_{j,1}, ..., a_{j,t}, ..., a_{j,n}, a_{j,n+1}, a_{j,n+2} \rangle$ Karena $A \in S$, $\overline{p_i p_j}$ bukan merupakan busur

dari $\overline{G}$. Sehingga partisipan p_i hanya memiliki $a_{i,i} = r_i$ dan nilai $a_{j,i}$ kosong, sedangkan partisipan p_j hanya memiliki $a_{j,j} = r_j$ dan nilai $a_{i,j}$ kosong.. Oleh karena itu mereka tidak dapat memperoleh informasi tentang y_i dan y_j. □

Teorema 4.1.3 (Sun dan Shieh, 1999)

Jika $A \in R$, maka A dapat menemukan *master key* dari konstruksi skema pembagian rahasia untuk Struktur Terlarang berdasarkan graf G.

Bukti:

Diasumsikan bahwa A={p_i,p_j}, dimana $i \neq j$. *Share* dari p_i adalah $S_i = \langle a_{i,1},...,a_{i,t},...,a_{i,n},a_{i,n+1},a_{i,n+2} \rangle$. Karena $A \in R$, $\overline{p_i p_j}$ merupakan busur dari $\overline{G}$ maka partisipan p_i memiliki $a_{i,i} = r_i$ dan $a_{i,j} = r_j + y_j$, partisipan p_j memiliki $a_{j,j} = r_j$ dan $a_{j,i} = r_j + y_i$ sehingga y_i dan y_j dapat diperoleh. Dari y_i dan y_j maka dpat diperoleh f(x) hingga akhirnya diperoleh *master key* K. □

Teorema 4.1.4 (Sun dan Shieh, 1999)

Jika $A \subseteq P$ dan $|A| \geq 3$, maka *A* dapat menemukan *master key* dari konstruksi skema pembagian rahasia untuk Struktur Terlarang berdasarkan graf G.

Bukti:

Tanpa menghilangkan keumumannya, diasumsikan bahwa A={p_i,p_j,p_k}, dimana i, j dan k berbeda. Jika terdapat sepasang partisipan yang merupakan elemen dari R, maka *master key* dapat ditemukan berdasarkan Teorema 3. Semua yang diperlukan untuk memandang kasus ini adalah bahwa semua $\overline{p_i p_j}$, $\overline{p_i p_k}$ dan $\overline{p_j p_k}$ adalah busur dari G. Jika $\overline{p_i p_j}$, $\overline{p_i p_k}$ dan $\overline{p_j p_k}$ busur dari G, maka p_i, p_j, dan $p_k \in T$. Oleh karena itu, partisipan p_i memiliki $a_{i,n+1} = s_{1,i}$ dan $a_{i,n+2} = s_{2,i}$; partispan p_j memiliki $a_{j,n+1} = s_{1,j}$ dan $a_{i,n+2} = s_{2,j}$; partisipan p_k memiliki $a_{k,n+1} = s_{1,k}$ dan $a_{k,n+2} = s_{2,k}$. Akibatnya p_i , p_j dan p_k dapat menemukan S_{k_1} dan S_{k_2} dimana $S_{k_1} = y_{n+1}$ dan $S_{k_2} = y_{n+2}$ sehingga dari y_{n+1} dan y_{n+2} diperoleh *master key K*. □

Untuk $|A| \geq 3$ karena selalu mempunyai subset *A'* dengan $|A'| = 2$, maka *A* selalu dapat merekonstruksi *master key K.*

Berdasarkan Teorema 4.1.1, Teorema 4.1.2, Teorema 4.1.3, dan Teorema 4.1.4 maka konstruksi dari skema pembagian rahasia dengan Struktur Terlarang tersebut memenuhi:

a) Jika $A \subseteq P$ dan $|A| > 2$, maka *A* tidak memperoleh informasi tentang *master key*.

b) Jika $A \in S$, maka *A* tidak memperoleh informasi tentang *master key*.

c) Jika $A \in R$, maka *A* dapat menemukan *master key*.

d). Jika $A \subseteq P$ dan $|A| \geq 3$, maka *A* dapat menemukan *master key*.

4.2 *Information rate*

Berikut ini akan dijelaskan tentang teorema-teorema yang digunakan untuk menentukan *information rate* pada skema pembagian rahasia untuk Struktur Terlarang.

Teorema 4.2.1(Sun dan Shieh, 1999)

Skema pembagian rahasia yang dibangun mempunyai *information rate* $2/(\bar{d}_{max}+3) \leq \rho \leq 2/(\bar{d}_{max}+1)$ jika $\bar{d}_{max} \leq n-3$, dimana $\bar{d}_{max}$ adalah derajat maksimum dari graf $\overline{G}$ dan n adalah jumlah simpul dari graf G.

Bukti:

Share dari partisipan p_i adalah $< a_{i,1},...,a_{i,t},...,a_{i,n},a_{i,n+1},a_{i,n+2} >$. Untuk n elemen pertama, jika $\overline{p_i p_j} \notin E(\overline{G})$ untuk $i \neq j$, $a_{i,j}$ adalah kosong. Untuk yang lain, $a_{i,j}$ adalah bilangan atas Z_q dan nilai $a_{i,i}$ tidak pernah kosong. Untuk dua elemen terakhir, $a_{i,n+1}$ dan $a_{i,n+2}$, masing-masing kosong atau merupakan bilangan atas Z_q. Oleh karena itu ukuran *share* S_i paling banyak $\log\left(q^{d_i+3}\right)$ (jika $a_{i,n+1}$ dan $a_{i,n+2}$ keduanya tidak kosong) dan paling sedikit $\log\left(q^{d_i+1}\right)$ (jika $a_{i,n+1}$ dan $a_{i,n+2}$ keduanya kosong), dimana d_i adalah derajat dari simpul p_i dari $\overline{G}$. Sehingga ukuran dari *share* paling banyak adalah $\log\left(q^{\bar{d}_{max}+3}\right)$ dan paling sedikit $\log\left(q^{\bar{d}_{max}+1}\right)$, dimana $\bar{d}_{max}$ adalah derajat maksimum dari $\overline{G}$. Karena ukuran

master key adalah $\log(q^2)$, *information rate* dari skema pembagian rahasia adalah $(2\times\log q)/((\overline{d}_{\max}+3)\times\log q) \le \rho \le (2\times\log q)/((\overline{d}_{\max}+1)\times\log q)$. Hingga akhirnya diperoleh $2/(\overline{d}_{\max}+3) \le \rho \le 2/(\overline{d}_{\max}+1)$. □

Teorema 4.2.2 (Sun dan Shieh, 1999)

Skema pembagian rahasia yang dikonstruksi mempunyai *information rate* $\rho = 2/(n-1)$ jika $\overline{d}_{\max} = n-2$, dimana $\overline{d}_{\max}$ adalah derajat maksimum dari $\overline{G}$ dan n adalah banyaknya simpul dari G.

Bukti:

Dengan mengikuti pembuktian dari Teorema 4.2.1, tanpa menghilangkan keumumannya, diasumsikan bahwa *share* dari partisipan p_i mempunyai ukuran maksimum diantara semua *share*. Sehingga d_i=n-2, dimana d_i adalah derajat dari simpul p_i dari $\overline{G}$. Akan ditunjukkan bahwa $p_i \notin T$ sebagai berikut: diasumsikan $p_i \in T$, maka terdapat p_j dan p_k sedemikian sehingga $\overline{p_i p_j}$ dan $\overline{p_i p_k} \notin \overline{G}$. Akibatnya derajat simpul p_i dari $\overline{G}$ paling banyak n-3. Hal ini kontradiksi dengan kenyataan bahwa d_i=n-2. Jadi $p_i \notin T$. Untuk n elemen pertama, terdapat $a_{i,j}$ sebanyak n-1 yang tidak kosong. Untuk dua elemen terakhir, $a_{i,n+1}$ dan $a_{i,n+2}$ keduanya kosong. Oleh karena itu, ukuran maksimal dari *share* adalah $\log(q^{n-1})$. Ukuran *master key* adalah $\log(q^2)$. Sehingga *information rate* dari skema pembagian rahasia yang dikonstruksi adalah $\rho = 2/(n-1)$. □

Teorema 4.2.3 (Sun dan Shieh, 1999)

Skema pembagian rahasia yang dikonstruksi mempunyai *information rate* $\rho = 2/n$ jika $\overline{d}_{\max} = n-1$, dimana $\overline{d}_{\max}$ adalah derajat maksimum dari $\overline{G}$ dan n adalah banyaknya simpul dari G.

Bukti:

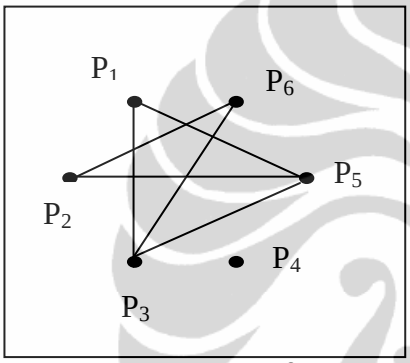
Mengikuti pembuktian dari Teorema 4.3.3. Karena d_i=n-1, semua nilai $a_{i,j}$ tidak kosong untuk $1 \le j \le n$ dan $a_{i,n+1}$ dan $a_{i,n+2}$ keduanya kosong. Oleh karena itu, *information rate* dari skema pembagian rahasia yang dikonstruksi adalah $\rho = 2/n$.

□

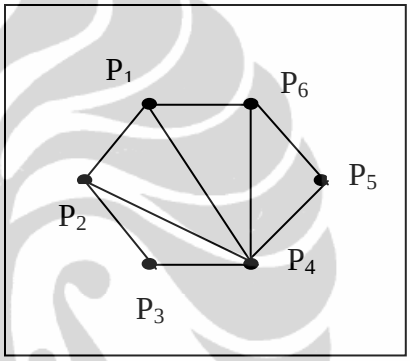
Dari Teorema 4.3.1, Teorema 4.3.2 dan Teorema 4.3.3 jelas bahwa batas bawah *information rate* dari skema pembagian rahasia yang dikonstruksi adalah $\max\{2/(\overline{d}_{\max}+3), 2/n\}$ dimana $\overline{d}_{\max}$ adalah derajat maksimum dari $\overline{G}$ dan n adalah banyaknya simpul dari G.

4.3 Contoh Konstruksi Untuk Struktur Terlarang

Berikut ini akan diberikan contoh konstruksi skema pembagaian rahasia untuk Struktur Terlarang dengan 6 partisipan yang dapat digambarkan dalam graf berikut.



Gambar 4.1. Graf G



Gambar 4.2. Graf $\bar{G}$

Berdasarkan Gambar 4.1 dan Gambar 4.2 diperoleh:

$P = \{p_1, p_2, p_3, p_4, p_5, p_6,\}$

$E(G) = \{\overline{p_1p_3}, \overline{p_1p_5}, \overline{p_2p_5}, \overline{p_2p_6}, \overline{p_3p_5}, \overline{p_3p_6}\}$

$E(\bar{G}) = \{\overline{p_1p_2}, \overline{p_1p_4}, \overline{p_1p_6}, \overline{p_2p_3}, \overline{p_2p_4}, \overline{p_3p_4}, \overline{p_4p_5}, \overline{p_4p_6}, \overline{p_5p_6}\}$

$S = \{\{p_1,p_3\}, \{p_1, p_5\}, \{p_2,p_5\}, \{p_2,p_6\}, \{p_3,p_5\}, \{p_3,p_6\}\}$

$R = \{\{p_1, p_2\}, \{p_1,p_4\}, \{p_1, p_6\}, \{p_2, p_3\}, \{p_2, p_4\}, \{p_3, p_4\}, \{p_4, p_5\}, \{p_4, p_6\}, \{p_5, p_6\}\}$

Struktur Terlarang dari skema pembagian rahasia yang direpresentasikan pada Gambar 4.1 adalah:

$\Delta_{\bar{G}} = \{\phi, \{p_1\}, \{p_2\}, \{p_3\}, \{p_4\}, \{p_5\}, \{p_6\}, \{p_1,p_3\}, \{p_1, p_5\}, \{p_2,p_5\}, \{p_2,p_6\}, \{p_3,p_5\}, \{p_3,p_6\}\}$

Struktur akses dari skema pembagian rahasia yang direpresentasikan pada Gambar 4.1 adalah:

$$\Gamma_{\bar{G}} = \{\{p_1, p_2\}, \{p_1, p_4\}, \{p_1, p_6\}, \{p_2, p_3\}, \{p_2, p_4\}, \{p_3, p_4\}, \{p_4, p_5\},$$
$$\{p_4, p_6\}, \{p_5, p_6\}, \{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_2, p_5\}, \{p_1, p_2, p_6\},$$
$$\{p_1, p_3, p_4\}, \{p_1, p_3, p_5\}, \{p_1, p_3, p_6\}, \{p_1, p_4, p_5\}, \{p_1, p_4, p_6\}, \{p_1, p_5, p_6\},$$
$$\{p_2, p_3, p_4\}, \{p_2, p_3, p_5\}, \{p_2, p_3, p_6\}, \{p_2, p_4, p_5\}, \{p_2, p_4, p_6\}, \{p_2, p_5, p_6\},$$
$$\{p_3, p_4, p_5\}, \{p_3, p_4, p_6\}, \{p_3, p_5, p_6\}, \{p_4, p_5, p_6\}, \{p_1, p_2, p_4, p_5\},$$
$$\{p_1, p_2, p_4, p_6\}, \{p_1, p_2, p_5, p_6\}, \{p_1, p_3, p_4, p_5\}, \{p_1, p_3, p_4, p_6\},$$
$$\{p_1, p_3, p_5, p_6\}, \{p_1, p_4, p_5, p_6\}, \{p_2, p_3, p_4, p_5\}, \{p_2, p_3, p_4, p_6\},$$
$$\{p_2, p_3, p_5, p_6\}, \{p_2, p_4, p_5, p_6\}, \{p_3, p_4, p_5, p_6\}, \{p_1, p_2, p_3, p_4, p_5\},$$
$$\{p_1, p_2, p_3, p_4, p_6\}, \{p_1, p_2, p_3, p_5, p_6\}, \{p_1, p_2, p_4, p_5, p_6\},$$
$$\{p_1, p_3, p_4, p_5, p_6\}, \{, p_2, p_3, p_4, p_5, p_6\}, \{p_1, p_2, p_3, p_4, p_5, p_6\}\}$$
$$T = \{p_1, p_3, p_5\}$$

Tahap Konstruksi Skema pembagian rahasia adalah sebagai berikut:

- **Langkah 1:**

  Tentukan q = 163. Misalkan diambil *master key* K= (K_1,K_2) = (3,2) dimana K_1 dan K_2 diambil secara acak dari Z_{163}

- **Langkah 2:**

  Dibentuk fungsi polinomial f(x) dalam Z_{163} sebagai berikut:

  $$f(x) = K_2 x + K_1 = 2x + 3$$

- **Langkah 3:**

  Hitung nilai y_i yang diperoleh dari f(x) dengan $y_i = f(i)$ untuk $i = 1, \ldots, 8$.

  Maka diperoleh

  $$y_1 = f(1) = 2.1 + 3 = 5$$
  $$y_2 = f(2) = 2.2 + 3 = 7$$
  $$y_3 = f(3) = 2.3 + 3 = 9$$
  $$y_4 = f(4) = 2.4 + 3 = 11$$
  $$y_5 = f(5) = 2.5 + 3 = 13$$
  $$y_6 = f(6) = 2.6 + 3 = 15$$
  $$y_7 = f(7) = 27 + 3 = 17$$
  $$y_8 = f(8) = 2.8 + 3 = 19$$

- **Langkah 4:**

  Dikonstruksi dua buah skema (3,6)-threshold dengan nama TS_1 dan TS_2, untuk memproteksi y_7 dan y_8.

  Master key dari TS_1 adalah Sk_1 yang disebut sebagai sub-*master key* dimana $Sk_1 = y_7$. *Master key* dari TS_2 adalah Sk_2 dimana $Sk_2 = y_8$.

  Share TS_1 disebut sub-*share* dari TS_1 yang terdiri dari $s_{1,1}, s_{1,2}, s_{1,3}, s_{1,4}, s_{1,5}, s_{1,6}$. Sedangkan *share* TS_2 disebut sub-*share* dari TS_2 yang terdiri dari $s_{2,1}, s_{2,2}, s_{2,3}, s_{2,4}, s_{2,5}, s_{2,6}$.

  Berikut ini adalah proses perhitungan untuk mencari nilai dari masing-masing sub*share* dari TS_1 dan TS_2.

  - Untuk (3,6)-TS_1:

    Sub *master key* dari TS_1 adalah $Sk_1=y_7=17$.

    Pilih dua bilangan acak atas Z_{163}, misalkan $a_{11} = 2$ dan $a_{12} = 3$. Kemudian dibentuk fungsi polynomial berderajat 2, yaitu

    $f_1(x) = a_{11}x^2 + a_{12}x + SK_1$ sehingga $f_1(x) = 2x^2 + 3x + 17$

    Maka sub*share* untuk TS_1 adalah:

    $$s_{1,1} = f_1(1) = 2.1^2 + 3.1 + 17 = 22$$
    $$s_{1,2} = f_1(2) = 2.2^2 + 3.2 + 17 = 31$$
    $$s_{1,3} = f_1(3) = 2.3^2 + 3.3 + 17 = 44$$
    $$s_{1,4} = f_1(4) = 2.4^2 + 3.4 + 17 = 61$$
    $$s_{1,5} = f_1(5) = 2.5^2 + 3.5 + 17 = 82$$
    $$s_{1,6} = f_1(6) = 2.6^2 + 3.6 + 17 = 107$$

  - Untuk (3,6)-TS_2:

    Sub *master key* dari TS_2 adalah $Sk_2=y_8=19$.

    Pilih dua bilangan acak atas Z_{163}, misalkan $a_{21} = 3$ dan $a_{22} = 5$. Kemudian dibentuk fungsi polynomial berderajat 2, yaitu

    $f_2(x) = a_{21}x^2 + a_{22}x + SK_2$ sehingga $f_2(x) = 3x^2 + 5x + 19$

    Maka sub*share* untuk TS_1 adalah:

    $$s_{2,1} = f_2(1) = 3.1^2 + 5.1 + 19 = 27$$
    $$s_{2,2} = f_2(2) = 3.2^2 + 5.2 + 19 = 41$$
    $$s_{2,3} = f_2(3) = 3.3^2 + 5.3 + 19 = 61$$

$$s_{2,4} = f_2(4) = 3.4^2 + 5.4 + 19 = 87$$
$$s_{2,5} = f_2(5) = 3.5^2 + 5.5 + 19 = 119$$
$$s_{2,6} = f_2(6) = 3.6^2 + 5.6 + 19 = 157$$

- **Langkah 5:**

  Pilih 6 bilangan acak atas Z_{163} misalkan

  $$r_1 = 2, r_2 = 3, r_3 = 5, r_4 = 7, r_5 = 11, r_6 = 13$$

- **Langkah 6:**

  Hitung *share* dari masing-masing partisipan dimana isi *share* dari p_i adalah $S_i = \langle a_{i,1}, \dots, a_{i,t}, \dots, s_{i,6} \rangle$ dimana $1 \leq t \leq 6$, dengan ketentuan:

  $$a_{i,t} = \begin{cases} r_i & \text{jika } t = i \\ r_i + y_i & \text{jika } t \neq i \ \overline{p_i p_t} \ \in E(\bar{G}) \\ \text{kosong} & \text{untuk yang lain} \end{cases}$$

  $$a_{i,7} = \begin{cases} s_{1,i} & p_i \in T \\ \text{kosong} & \text{untuk yang lain} \end{cases}$$

  $$a_{i,8} = \begin{cases} s_{2,i} & p_i \in T \\ \text{kosong} & \text{untuk yang lain} \end{cases}$$

  Berdasarkan ketentuan di atas, *share* dari masing masing partisipan dapat dilihat pada Tabel 4.1 dan Tabel 4.2 berikut.

i	S_i	$a_{i,1}$	$a_{i,2}$	$a_{i,3}$	$a_{i,4}$	$a_{i,5}$	$a_{i,6}$	$a_{i,7}$	$a_{i,8}$
1	S_1	r_1	r_2+y_2	-	r_4+y_4	-	r_6+y_6	$s_{1,1}$	$s_{2,1}$
2	S_2	r_1+y_1	r_2	r_3+y_3	r_4+y_4	-	-	-	-
3	S_3	-	r_2+y_2	r_3	r_4+y_4	-	-	$s_{1,3}$	$s_{2,3}$
4	S_4	r_1+y_1	r_2+y_2	r_3+y_3	r_4+y_4	r_5+y_5	r_6+y_6	-	-
5	S_5	-	-	-	r_4+y_4	r_5	r_6+y_6	$s_{1,5}$	$s_{2,5}$
6	S_6	r_1+y_1	-	-	r_4+y_4	r_5+y_5	r_6	-	-

Tabel 4.1 Isi *share* dari masing-masing partisipan

i	S_i	$a_{i,1}$	$a_{i,2}$	$a_{i,3}$	$a_{i,4}$	$a_{i,5}$	$a_{i,6}$	$a_{i,7}$	$a_{i,8}$
1	S_1	22	10	-	18	-	28	22	27
2	S_2	7	3	14	18	-	-	-	-
3	S_3	-	10	5	18	-	-	44	61
4	S_4	7	10	14	7	24	28	-	-
5	S_5	-	-	-	18	11	28	82	119
6	S_6	7	-	-	18	24	13	-	-

Tabel 4.2 Nilai *share* dari masing-masing partisipan

Berikut ini akan diperlihatkan bahwa skema pembagian rahasia untuk Struktur Terlarang yang dibangun memenuhi:

a) Jika $A \subseteq P$ dan $|A| = 1$, maka A tidak memperoleh informasi tentang *master key*

Misalkan diambil $A = \{p_4\} \in \Delta$. Dari tabel 4.1 dan tabel 4.2 diperoleh:

$$S_4 = \langle r_1 + y_1, r_2 + y_2, r_3 + y_3, r_4, r_5 + y_5, r_6 + y_6, -, - \rangle = < 7, 10, 14, 7, 24, 28, -, - >$$

Dari isi *share* S_4 terlihat bahwa p_4 tidak memperoleh nilai y_i manapun, sehingga *master key* tidak dapat direkonstruksi. Dengan cara yang sama dapat ditunjukkan bahwa sifat a) juga berlaku untuk p_i yang lain.

b) Jika $A \in S$, maka A tidak memperoleh informasi tentang *master key*.

Misalkan diambil $A = \{p_1, p_3\} \in \Delta$, dari Tabel 4.1 dan Tabel 4.2 diperoleh:

$$S_1 = \langle r_1, r_2 + y_2, r_3, r_4 + y_4, -, r_6 + y_6, s_{1,1}, s_{2,1} \rangle = < 2, 10, -, 18, -, 28, 22, 27 >$$

$$S_3 = \langle -, r_2 + y_2, r_3, r_4 + y_4, -, -, s_{1,3}, s_{2,3} \rangle = < -, 10, 5, 18, -, -, 44, 61 >$$

Dari isi *share* S_1 dan S_2 terlihat bahwa p_1 dan p_3 tidak memperoleh nilai y_1 dan y_2 ataupun y_i yang lain, sehingga *master key* tidak dapat direkonstruksi

c) Jika $A \in R$, maka A dapat menemukan *master key*

Misalkan diambil $A = \{p_1, p_2\} \in \Gamma$. Dari Tabel 4.1 dan Tabel 4.2 diperoleh:

$$S_1 = \langle r_1, r_2 + y_2, r_3, r_4 + y_4, -, r_6 + y_6, s_{1,1}, s_{2,1} \rangle = < 2, 10, -, 18, -, 28, 22, 27 >$$

$$S_2 = \langle r_1 + y_1, r_2, r_3 + y_3, r_4 + y_4, -, -, -, - \rangle = < 7, 3, 14, 18, -, -, -, - >$$

Dari S_1 dan S_2, p_1 dan p_2 memperoleh nilai $r_1, r_2, r_1 + y_1, r_2 + y_2$ yang dapat digunakan untuk mencari nilai y_1 dan y_2, sehingga akan ditemukan *master key* K.

Proses perhitungannya adalah sebagai berikut:

$r_1 = 2,\ r_1 + y_1 = 7$ maka $y_1 = 5 = K_2.1 + K_1$

$r_2 = 3,\ r_2 + y_2 = 10$ maka $y_2 = 7 = K_2.2 + K_1$ +

$-2 = -K_2$ maka

$K_2 = 2 \rightarrow K_2 + K_1 = 5$ maka $K_1 = 3$.

Maka diperoleh *master key* $K = (K_1, K_2) = (3,2)$.

d) Jika $A \subseteq P$ dan $|A| \geq 3$, maka A dapat menemukan *master key*.

Jika $A = \{p_1, p_3, p_5\} \in \Gamma$, A akan dapat menemukan *master key* K karena:

$S_1 = \langle r_1, r_2 + y_2, r_3, r_4 + y_4, -, r_6 + y_6, s_{1,1}, s_{2,1} \rangle = < 2,10,-,18,-,28,22,27 >$

$S_3 = \langle -, r_2 + y_2, r_3, r_4 + y_4, -, -, s_{1,3}, s_{2,3} \rangle = < -,10,5,18,-,-,44,61 >$

$S_5 = \langle -, -, -, r_4 + y_4, r_5, r_6 + y_6, s_{1,5}, s_{2,5} \rangle = < -, -, -,18,11,28,82,119 >$

Dari S_1, S_2 dan S_3 dapat diperoleh $s_{1,1}, s_{1,3}, s_{1,5}, s_{2,1}, s_{2,3}, s_{2,5}$ dimana $s_{1,1}, s_{1,3}, s_{1,5}$ dapat digunakan untuk mencari SK_1 dan $s_{2,1}, s_{2,3}, s_{2,5}$ dapat digunakan untuk mencari SK_2.

Karena $SK_1 = y_7$ dan $SK_2 = y_8$, maka dari y_7 dan y_8 dapat diperoleh *master key* K. Proses perhitungannya adalah sebagai berikut:

dengan menggunakan polinomial interpolasi Lagrange

$$f(x) = \sum_{k=1}^{n} \left(f_k . l_k(x)\right) \text{ dengan } l_k(x) = \prod_{j=1, j \neq k}^{n} \frac{(x - x_j)}{x_k - x_j}$$

Untuk mencari SK_1 diketahui $s_{1,1} = 22,\ s_{1,3} = 44, s_{1,5} = 82.$ Misalkan $f_1 = s_{1,1} = 22,\ f_2 = s_{1,3} = 44, f_3 = s_{1,5} = 82,$ maka

$$l_1(x) = \prod_{j=1, j \neq 1}^{3} \frac{(x - x_j)}{(1 - x_j)} = \frac{(x - x_2)}{(1 - x_2)} \frac{(x - x_3)}{(1 - x_3)} = \frac{(x - 3)}{(1 - 3)} \frac{(x - 5)}{(1 - 5)} = \frac{1}{8}(x^2 - 8x + 15)$$

$$l_2(x) = \prod_{j=1, j \neq 1}^{3} \frac{(x - x_j)}{(3 - x_j)} = \frac{(x - x_1)}{(3 - x_1)} \frac{(x - x_3)}{(3 - x_3)} = \frac{(x - 1)}{(3 - 1)} \frac{(x - 5)}{(3 - 5)} = \frac{1}{-4}(x^2 - 6x + 5)$$

$$l_3(x) = \prod_{j=1, j\neq 1}^{3} \frac{(x-x_j)}{(5-x_j)} = \frac{(x-x_1)}{(5-x_1)}\frac{(x-x_2)}{(5-x_2)} = \frac{(x-1)}{(5-1)}\frac{(x-3)}{(5-3)} = \frac{1}{8}(x^2-4x+3)$$

Sehingga

$$\begin{aligned} f(x) &= \textstyle\sum_{k=1}^{3}\left(f_k . l_k(x)\right) \\ &= f_1 . l_1(x) + f_2 . l_2(x) + f_3 . l_3(x) \\ &= 22.\tfrac{1}{8}(x^2-8x+15) + 44.\tfrac{1}{-4}(x^2-6x+5) + 82.\tfrac{1}{8}(x^2-4x+3) \\ &= \left(22.\tfrac{1}{8} - 44.\tfrac{1}{4} + 82.\tfrac{1}{8}\right)x^2 + \left(22.\tfrac{1}{8}(-8) - 44.\tfrac{1}{4}(-6) + 82.\tfrac{1}{8}(-4)\right)x + \\ &\quad \left(22.\tfrac{1}{8}.15 - 44.\tfrac{1}{4}.5 + 82.\tfrac{1}{8}.3\right) \\ f(x) &= 2x^2 + 3x + 17 = a_{11}x^2 + a_{12}x + SK_1 \end{aligned}$$

Sehingga diperoleh $SK_1 = 17$

Untuk mencari SK_2 diketahui $s_{2,1} = 27,\ s_{2,3} = 61, s_{2,5} = 119$, Misalkan $f_1 = s_{2,1} = 27,\ f_2 = s_{2,3} = 61, f_3 = s_{2,5} = 119,$ maka

$$l_1(x) = \prod_{j=1, j\neq 1}^{3} \frac{(x-x_j)}{(1-x_j)} = \frac{(x-x_2)}{(1-x_2)}\frac{(x-x_3)}{(1-x_3)} = \frac{(x-3)}{(1-3)}\frac{(x-5)}{(1-5)}$$

$$= \frac{1}{8}(x^2-8x+15)$$

$$l_2(x) = \prod_{j=1, j\neq 1}^{3} \frac{(x-x_j)}{(3-x_j)} = \frac{(x-x_1)}{(3-x_1)}\frac{(x-x_3)}{(3-x_3)} = \frac{(x-1)}{(3-1)}\frac{(x-5)}{(3-5)}$$

$$= \frac{1}{-4}(x^2-6x+5)$$

$$l_3(x) = \prod_{j=1, j\neq 1}^{3} \frac{(x-x_j)}{(5-x_j)} = \frac{(x-x_1)}{(5-x_1)}\frac{(x-x_2)}{(5-x_2)} = \frac{(x-1)}{(5-1)}\frac{(x-3)}{(5-3)}$$

$$= \tfrac{1}{8}(x^2-4x+3)$$

Sehingga

$$\begin{aligned} f(x) &= \textstyle\sum_{k=1}^{3}\left(f_k . l_k(x)\right) = f_1 . l_1(x) + f_2 . l_2(x) + f_3 . l_3(x) \\ &= 27.\tfrac{1}{8}(x^2-8x+15) + 61.\tfrac{1}{-4}(x^2-6x+5) + 119.\tfrac{1}{8}(x^2-4x+3) \\ &= \left(27.\tfrac{1}{8} - 61.\tfrac{1}{4} + 119.\tfrac{1}{8}\right)x^2 + (27.\tfrac{1}{8}(-8) - 61.\tfrac{1}{4}(-6) \\ &\quad +110.\tfrac{1}{8}(-4))x + \left(27.\tfrac{1}{8}.15 - 61.\tfrac{1}{4}.5 + 119.\tfrac{1}{8}.3\right) \\ f(x) &= 3x^2 + 5x + 19 = a_{21}x^2 + a_{22}x + SK_2 \end{aligned}$$

Sehingga diperoleh $SK_2 = 19$.

$SK_1 = y_7 = 17 = K_2.7 + K_1$

$SK_2 = y_8 = 19 = K_2.8 + K_1$

$-2 = -K_2$ maka $K_2 = 2 \rightarrow K_2 + K_1 = 5$ maka $K_1 = 3$.

Sehingga diperoleh *master key* $K = (K_1, K_2) = (3,2)$.

Berikut ini akan dihitung *information rate* dari contoh konstruksi skema pembagian rahasia yang dibuat.

- BerdasarkanTabel 4.1 terlihat bahwa ukuran *share* S_i dari masing-masing partisipan dengan i=1,...,6 adalah: $|S_1| = 6, |S_2| = 4, |S_3| = 5, |S_4| = 6, |S_5| = 5, |S_6| = 4$.

  Ukuran dari *master key* adalah $|K| = 2$ .Maka berdasarkan berdasarkan [Brickell dan Davenport, 1991], *information rate*nya adalah:

$$\rho = \frac{log_2|K|}{\max_i \log_2|S_i|} = \frac{log_2|2^8|^2}{log_2|2^8|^6} = \frac{2.log_2|2^8|}{6.log_2|2^8|} = \frac{1}{3}$$

- Dari Gambar 4.2 terihat bahwa $\bar{d}_{\max} = 5 = 6 - 1 = n - 1$, maka berdasarkan Teorema 4.2.3 *information rate*nya adalah:

$$\rho = \frac{2}{n} = \frac{2}{6} = \frac{1}{3}$$

Dari hasil kedua perhitungan diatas, nilai *information rate* yang diperoleh adalah sama. Pada perhitungan *information rate* berdasarkan [Brickell dan Davenport, 1991], dimana untuk mencari ukuran maksimal dari *share*-nya harus melihat satu per satu dari masing-masing *share*, baru kemudian dihitung rasionya, sedangkan pada perhitungan berdasarkan [Sun & Shieh, 1997] hanya cukup melihat dari struktur grafnya Sehingga dapat dikatakan bahwa proses perhitungan *information rate* berdasarkan Sun & Shieh lebih sederhana jika dibandingkan berdasarkan [Brickell dan Davenport, 1991].

Berdasarkan penjelasan dari Bab 3 dan Bab 4, pada bab berikutnya akan dijelaskan mengenai analisis perbandingan dari kedua skema tersebut.

BAB 5
ANALISIS PERBANDINGAN SKEMA PEMBAGIAN RAHASIA UNTUK STRUKTUR AKSES DAN STRUKTUR TERLARANG BERDASARKAN GRAF

Berdasarkan penjelasan pada Bab 4 dan Bab 5, berikut ini akan diberikan hasil perbandingan antara skema pembagian rahasia untuk struktur akses dan struktur terlarang berdasarkan graf.

5.1 Persamaan

Berikut ini adalah beberapa persamaan yang dimiliki oleh skema pembagian rahasia untuk struktur akses dan struktur terlarang berdasarkan graf.

a) Menggunakan himpunan partisipan $P = \{p_1, p_2, \ldots, p_n\}$ yang masing-masing partisipan direpresentasikan sebagai sebuah simpul dalam graf G
b) Menggunakan bilangan bulat modulo q (Z_q)
c) Menggunakan *master key* yang terdiri dari dua elemen.
d) Menggunakan fungsi polinomial berderajat satu dengan koefisien-koefisien yang diambil dari elemen *master key* untuk menghitung nilai y_i.

5.2 Perbedaan

Berikut ini adalah beberapa perbedaan yang dimiliki oleh skema pembagian rahasia untuk struktur akses dan struktur terlarang berdasarkan graf, yang ditunjukkan pada Tabel 5.1.

No.	Skema Pembagian Rahasia Struktur Akses	Skema Pembagian Rahasia Struktur Terlarang
1.	**Parameter yang digunakan:** a. S adalah himpunan pasangan partisipan yang dihubungkan dengan busur, yang dapat merekonstruksi *master key* b. Tidak perlu himpunan R.	a. S adalah himpunan pasangan partisipan yang dihubungkan dengan busur dalam graf G, yang tidak dapat merekonstruksi *master key* b. R adalah himpunan pasangan partisipan yang dihubungkan dengan busur dalam graf $\overline{G}$, yang dapat merekonstruksi *master key*

No.	Skema Pembagian Rahasia Struktur Akses	Skema Pembagian Rahasia Struktur Terlarang
	c.Struktur Akses Γ dinyatakan dengan $\Gamma = \{B \subseteq P \mid B \supseteq A, A \in S\}$ d. Struktur Terlarang Δ dinyatakan dengan $\Delta = 2^P \setminus \Gamma = \{A \subseteq P \mid B \not\subset A \text{ untuk semua } B \in S\}$ e. Tidak memerlukan himpunan T	c. Struktur Akses Γ dinyatakan dengan $2^P \setminus \Delta = \{A \mid A \subseteq P \text{ dan } \lvert A \rvert \geq 3\} \cup \{A \mid A \in R\}$ d. Struktur Terlarang Δ dinyatakan dengan $\Delta = \{A \mid A \subseteq P \text{ dan } \lvert A \rvert = 1\} \cup \{A \mid A \in S\}$ e. Menggunakan T yang dinyatakan dengan $T = \{p_i : \exists p_j \text{ dan } p_k \ni \overline{p_i p_j}, \overline{p_i p_k}$ dan $\overline{p_j p_k} \in E(G), i \neq j \neq k\}$
2.	**Kunci yang digunakan:** Terdapat satu jenis kunci yang digunakan, yaitu *master key* yang terdiri dari dua elemen	Terdapat dua jenis kunci yang digunakan, yaitu *master key* dan *submaster key* yang masing-masing terdiri dari dua elemen
3.	**Penggunaan bilangan acak:** Bilangan acak yang digunakan sebanyak n+2 buah	Bilangan acak yang digunakan sebanyak n+6 buah
4.	**Share:** a. Merupakan sebuah vektor yang terdiri dari n elemen, yaitu: $S_i = \langle a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n} \rangle$ b. Ketentuan isi share: $a_{i,t} = \begin{cases} r_i & \text{jika } t = i \\ r_t + y_t & \text{jika } t \neq i \text{ dan } \overline{p_i p_t} \in \text{E(G)} \\ \text{kosong} & \text{jika } t \neq i \text{ dan } \overline{p_i p_t} \notin \text{E(G)} \end{cases}$ c. Tidak menggunakan skema (t,n) *threshold* d. Isi share mengandung bilangan acak r_i dan nilai y_i	a. Merupakan sebuah vektor yang terdiri dari n+2 elemen, yaitu: $S_i = \langle a_{i,1}, \ldots, a_{i,t}, \ldots, a_{i,n}, a_{i,n+1}, a_{i,n+2} \rangle$ b. Ketentuan isi share: $a_{i,t} = \begin{cases} r_i & \text{jika } t = i \\ r_i + y_i & \text{jika } t \neq i \ \overline{p_i p_t} \in E(\bar{G}) \\ \text{kosong} & \text{untuk yang lain} \end{cases}$ $a_{i,7} = \begin{cases} s_{1,i} & p_i \in T \\ \text{kosong} & \text{untuk yang lain} \end{cases}$ $a_{i,8} = \begin{cases} s_{2,i} & p_i \in T \\ \text{kosong} & \text{untuk yang lain} \end{cases}$ c. Diperlukan dua buah skema (3,n) *threshold* d. Isi share mengandung bilangan acak r_i , nilai y_i dan *subshare* dari TSi

No.	Skema Pembagian Rahasia Struktur Akses	Skema Pembagian Rahasia Struktur Terlarang
	e. Tidak mempunyai *subshare*	e. Mempunyai *subshare* yang dibangun menggunakan dua skema (3,n) *threshold*
5.	**Sifat struktur akses** Struktur akses Γ monoton naik	Struktur akses Δ monoton turun
6.	**Graf yang digunakan** a.Menggunakan graf G b.Dua simpul yang dihubungkan dengan busur dapat merekonstruksi *master key* K	a.Menggunakan graf G dan komplemen G $(\overline{G})$ b.Dua simpul yang dihubungkan dengan busur tidak dapat merekonstruksi *master key* K
7.	***Information Rate:*** Dihitung berdasarkan derajat maksimum dari graf G ($d_{\max}$) dengan rumus $\rho = \frac{2}{d_{\max}+1}$	Dihitung berdasarkan derajat maksimum dari graf $\overline{G}$ ($\overline{d}_{\max}$) dengan rumus $2/(\overline{d}_{\max}+3) \le \rho \le 2/(\overline{d}_{\max}+1)$, jika $\overline{d}_{\max} \le n-3$ $\rho = 2/(n-1)$ jika $\overline{d}_{\max} = n-2$ $\rho = 2/n$ jika $\overline{d}_{\max} = n-1$

Tabel 5.1 Perbedaan Skema Pembagian Rahasia untuk Struktur Akses dan Struktur Terlarang

Berdasarkan Teorema 3.1.2 dan Teorema 3.1.3 terlihat bahwa pada skema untuk Struktur Akses, tidak setiap himpunan partisipan yang terdiri dari dua elemen atau lebih akan dapat merekonstruksi rahasia, Sedangkan berdasarkan Teorema 4.1.4 terlihat bahwa pada skema untuk.Struktur Telarang jika setiap himpunan partisipan yang terdiri dari tiga elemen atau lebih selalu dapat merekonstruksi rahasia. Sehingga dapat dikatakan bahwa pada Struktur Terlarang jika banyaknya himpunan partisipan lebih besar atau sama dengan tiga, maka himpunan partisipan tersebut selalu dapat merekonstruksi *master key*, tetapi pada Struktur Akses sifat ini belum tentu berlaku. Akibatnya kedua struktur tersebut tidak saling komplemen, meskipun jika dilihat dari struktur grafnya terlihat bahwa graf yang menyatakan akses struktur dari kedua skema saling komplemen.

BAB 6
KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan penjelasan dari bab-bab sebelumnya, dapat diambil beberapa kesimpulan sebagai berikut:

a) Sebuah busur pada skema pembagian rahasia untuk struktur akses menunjukkan bahwa dua partisipan dapat merekonstruksi *master key*, tetapi pada struktur terlarang justru sebaliknya. Sehingga dalam melakukan konstruksi maupun perhitungan *information rate* harus diperhatikan struktur graf dan komplemennya..
b) Banyaknya elemen *share* pada Struktur Terlarang lebih besar dibandingkan pada Struktur Akses. Elemen tambahan pada Struktur Terlarang digunakan untuk menjamin bahwa himpunan partisipan yang lebih dari 3 selalu dapat merekonstruksi *master key*.
c) *Information rate* pada Struktur Terlarang maupun pada Struktur Akses, tidak dapat langsung dibandingkan dan sangat bergantung pada struktur grafnya..
d) Proses konstruksi pada skema pembagian rahasia untuk struktur akses lebih sederhana jika dibandingkan pada Struktur Akses.
e) Kedua skema bukan merupakan skema yang saling komplemen satu sama lain meskipun grafnya saling komplemen.

6.2 Saran

Untuk penelitian lanjutan dapat dilihat kemungkinan membangun konstruksi baru yang merupakan perluasan ataupun modifikasi dari konstruksi yang ada baik untuk struktur akses ataupun untuk struktur terlarang.

DAFTAR PUSTAKA

Brickell, E.F dan Stinson, D. R. (1990) Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes. *Crypto'90,*pp.242-252

Brickell, E.F and Davenport, D. M. (1991): On The Classification of Ideal Secret Sharing Schemes. *Journal of Cryptology* 4:2 123-134.

Capocelli, R. M., et al. (1993) On The Size of Shares for Secret Sharing Schemes. *Journal of Cryptology* 6: 3: 157-167.

Ito, Mitsuro., Saito, Akira., dan Nishizeki, Takao. (1987) Secret Sharing Scheme Realizing General Access Structure. *Proc. of IEEE Globecom'87, Tokyo*: 99-102.

Jackson W.A., Martin K.M., O'Keefe C.M., (1994) Multisecret Threshod Schemes. *Advance in Cryptology-Crypto '93 Proceedings. Lecture Notes in Computer Science,* 773. Berlin: Springer Verlag, 1994. P. 126-35.

Karnin, E. D., Green, J. W., Hellman, M. E. (1992). On Secret Sharing Systems, *IEEE Trans* IT-29: 1 (1992): 35-41.

Martana, I K. T., dan Indah, Retno. (2010) Ukuran Share pada Konstruksi Pembagian Rahasia, *Prosiding Seminar Nasional Matematika UI-Unpad 2010,* Depok.

Rosen, K. H. (1999). .*Discrete Mathematics and Its Applications*. Fourth Editions. New York: CRC Pres.

Shamir, A. (1979): How to Share a Secret. *Communications of the ACM,* 22: 11 612-613.

Stinson, D.R. (1992) New Genersl Bounds On The Information Rate of Secret Sharing Schemes, *Crypto'92*.

Sun, H. M., dan Shieh, S. P. [1999] Constructing Perfect Secret Sharing Schemes for General And Uniform Access Structures. *Journal of Information Science And Engineering 15,679-689*

Sun, H. M., [1999] New Construction of Perfect Secret Sharing Schemes for Graph-based prohibited Structures for General And Uniform Access Structures. *Journal of Computers and Electrical* 25,267-277.

Sun, H. M., dan Shieh, S. P. (1997) Secret Sharing in Graph-based Prohibited Structures. *Proceeding of IEEE INFOCOM'97*: 718-724.

Wang, Y.C. dan Juan, J. S. (2007) A Perfect Secret Sharing Scheme for r-Uniform Hypergraph-Based Access Structures. *Proceeding of The 24rd Workshop on Combinatorial Mathematics and Computation Theory*: (2007): 28-34.

Wilson, R. J. (1996) *Introduction to Graph Theory*. Fourth Edition Longman Group Ltd. England