UNIVERSITAS INDONESIA

ANALISIS PERBANDINGAN SKEMA PEMBAGIAN RAHASIA 3-STRUKTUR AKSES HIPERGRAF DAN 3-STRUKTUR TERLARANG HIPERGRAF

TESIS

I KETUT TRI MARTANA
0806420215

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

UNIVERSITAS INDONESIA

ANALISIS PERBANDINGAN SKEMA PEMBAGIAN RAHASIA 3-STRUKTUR AKSES HIPERGRAF DAN 3-STRUKTUR TERLARANG HIPERGRAF

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Sains

I KETUT TRI MARTANA
0806420215

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	: I Ketut Tri Martana
NPM	: 0806420215
Tanda Tangan	:
Tanggal	: 8 Juli 2010

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :

Nama	: I Ketut Tri Martana
NPM	: 0806420215
Program Strudi	: Magister Matematika
Judul Tesis	: Analisis Perbandingan Skema Pembagian Rahasia 3-Struktur Akses Hipergraf dan 3-Struktur Terlarang Hipergraf

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

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat rahmat-Nya, Tesis ini dapat saya 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.

Saya 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, saya mengucapkan terima kasih kepada:

(1) Dr. Kiki Ariyanti Sugeng, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan Tesis ini;
(2) Dr. Yudi Satria, M.T, selaku ketua Departemen Matematika FMIPA UI dan Rahmi Rusin S.Si, M.Sc.Tech, selaku Sekretaris Departemen Matematika FMIPA UI;
(3) Prof. Dr. Djati Kerami, selaku ketua Program Magister Matematika FMIPA UI dan Dra. Bevina Desjwiandra H M.Sc, Ph.D, selaku skretaris sekaligus pembimbing akademis pada Program Magister Matematika FMIPA UI;
(4) Para dosen pada Program Magister Matematika FMIPA UI yang telah memberikan arahan dan bimbingan selama perkuliahan;
(5) Lembaga Sandi Negara, institusi saya yang telah memberikan kesempatan dan dukungan dalam perkuliahan dan penyelesaian Tesis ini;
(6) Orang tua dan keluarga besar saya, yang telah memberikan dukungan moral, materiil serta doa yang tidak pernah berhenti;
(7) Istri tercinta, atas segala dukungan, semangat dan doanya;
(8) Teman seperjuangan angkatan 2008 yang selalu kompak dan telah membantu dalam segala hal;
(9) Rekan-rekan kerja baik pada Lembaga Sandi Negara maupun Sekolah Tinggi Sandi Negara, atas segala bantuan dan dukungannya;
(10) Berbagai pihak yang tidak dapat disebutkan satu per satu yang telah membantu penyelesaian Tesis ini.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Akhir kata, saya 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

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama	: I Ketut Tri Martana
NPM	: 0806420215
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
3-Struktur Akses Hipergraf dan 3-Struktur Terlarang Hipergraf

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Biaya Royalti Noneksklusif ini Universitas Indonesia berhak untuk 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:

(I Ketut Tri Martana)

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

ABSTRAK

Nama : I Ketut Tri Martana
Program Studi : Magister Matematika
Judul : Analisis Perbandingan Skema Pembagian Rahasia 3-Struktur Akses Hipergraf dan 3-Struktur Terlarang Hipergraf

Akses terhadap informasi rahasia perlu diatur dan dibatasi supaya tidak jatuh kepada pihak yang tidak berkepentingan. Salah satu metode yang mengatur akses tersebut adalah skema pembagian rahasia. Skema pembagian rahasia merupakan suatu skema dimana hanya anggota kelompok (partisipan) dengan kualifikasi tertentu saja yang dapat merekonstruksi informasi rahasia. Koleksi dari subset partisipan yang berkualifikasi disebut struktur akses. Skema pembagain rahasia yang dapat direpresentasikan dengan graf disebut sebagai skema pembagian rahasia *graphical*. Skema ini dapat diperluas dengan menggunakan hipergraf, yang merupakan bentuk lebih umum dari graf. Skema yang direpresentasikan dengan hipergraf adalah salah satu bentuk dari skema pembagian rahasia *non-graphical*. Tesis ini akan membahas mengenai perbandingan dari skema pembagian rahasia yang berdasarkan struktur akses Γ dan srtuktur terlarang Δ pada hipergraf 3-*uniform* serta *information rate* dari kedua konstruksi skema pembagian rahasia.

Kata kunci : Skema Pembagian Rahasia, Struktur Akses, *Information Rate*
xi+63 halaman; 8 gambar; 5 tabel
Daftar Pustaka : 16 (1979-2010)

ABSTRACT

Name : I Ketut Tri Martana
Study Program : Magister of Mathematics
Title : Comparison Analysis of Secret Sharing Scheme of 3-Hipergraph Access and 3-Hipergraph Prohibited

Access for secret information shall be limited and arranged that not be accepted to not important people. One of the method to arranged this access is secret sharing scheme. Secret sharing scheme is a method which allow a secret to be share among a set of participants in such a way that only qualified subsets or participant can recover the secret. The collection of qualified subsets is called access structure. The scheme that can be represented by graph is called graphical secret sharing scheme. More general from graph, represented by hypergraph, is one of the scheme called non graphical secret sharing scheme. In this thesis will presents the comparison analysis of secret sharing scheme between access structure Γ and prohibited structure Δ based on 3-uniform hypergraph, including the information rate of that schemes.

Key words : Secret Sharing Scheme, Access Structures, Information Rate
xi+63 pages; 8 pictures; 5 tables
Bibliography : 16 (1979-2010)

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

DAFTAR ISI

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

DAFTAR TABEL

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

DAFTAR GAMBAR

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

BAB 1
PENDAHULUAN

Bagian Pendahuluan dari Tesis ini akan memuat mengenai latar belakang dilakukannya penelitian, permasalahan yang akan dikaji, tujuan penulisan, batasan masalah dan sistematika penulisan. Berikut ini adalah uraian selengkapnya.

1.1 Latar Belakang

Keamanan data (*data security*) menjadi hal yang sangat penting dewasa ini, terutama informasi yang bersifat rahasia (*secret*). Contohnya data-data negara mengenai kebijakan strategis; seperti keamanan dan kepentingan nasional, data suatu perusahaan atau perbankan; seperti data nasabah, data aliran dana / modal dan lain sebagainya. Data penting tersebut perlu mendapat perlakuan pengamanan yang memadai, supaya tidak bocor kepada pihak yang tidak berkepentingan. Misalnya data rahasia negara jika jatuh ke tangan negara lain, maka secara otomatis akan memanfaatkannya sebagai dasar pengambilan kebijakan nasional suatu negara yang mungkin saja merugikan negara kita. Data perbankan juga sangat bernilai strategis, akan terjadi gangguan dalam bidang ekonomi jika data perbankan yang bersifat rahasia bocor pada pihak yang tidak berkepentingan.

Terkadang keamanan data hanya diserahkan kepada satu orang saja sebagai penanggung jawab. Permasalahan timbul ketika orang yang bertanggung jawab untuk membuka atau mengakses data tersebut berhalangan, tidak ditempat atau meninggal dunia, maka data tidak bisa diakses.

Sebagai contoh, data nasabah suatu bank merupakan data penting yang perlu dirahasiakan, umumnya data tersebut disimpan pada komputer utama di kantor pusat. Pada saat yang sama data tersebut juga tersimpan pada kantor cabang tertentu, seandainya ada suatu bencanan alam yang dapat merusak sistem pada komputer pusat, maka data pada kantor cabang masih bisa digunakan. Namun menyimpan semua data secara lengkap pada kantor cabang juga sangat berbahaya karena tingkat keamanannya tidak sekuat

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

sistem pengamanan komputer pusat. Untuk itu pengaturan akses tehadap data rahasia perlu mendapat perhatian khusus sehingga diketahui secara pasti siapa saja yang berhak untuk mengakses dan memperoleh data rahasia. Tujuan utamanya adalah keamanan data rahasia bisa terjamin.

Pengamanan data dalam Kriptografi menggunakan proses enkripsi dan dekripsi. Enkripsi merupakan proses penyandian berita rahasia, sedangkan dekripsi adalah proses membuka sandi berita rahasia. Proses enkripsi dan dekripsi tersebut menggunakan kunci rahasia. Pengamanan kunci rahasia juga mutlak harus diperhatikan, dalam hal ini diperlukan pengaturan akses terhadap kunci rahasia tersebut.

Salah satu metode dalam pengaturan akses dan pembagian (*sharin*g) data rahasia yang sering digunakan adalah konsep Skema Pembagian Rahasia (*secret sharing scheme*). Dalam skema pembagian rahasia, akses terhadap informasi rahasia diberikan kepada beberapa orang dengan kualifikasi tertentu, misalnya n orang, maka dalam merekonstruksi suatu data rahasia dibutuhkan minimal k-orang tersebut, dimana $k \leq n$. Apabila kurang dari k maka data rahasia tidak bisa direkonstruksi.

Saat ini, skema pembagian rahasia telah dipelajari secara luas. Hal ini karena aplikasinya dapat diterapkan pada berbagai bidang yang berhubungan dengan pengamanan data / informasi dan kriptografi, misalnya pada manajemen kunci rahasia, pengamanan perbankan, *e-commerce*, proses penawaran dalam lelang (*bidding*), keamanan jaringan komputer (*network security*), dan lain sebagainya.

Skema pembagian rahasia pertama kali diperkenalkan oleh A. Shamir dan G. Blackley pada tahun 1979 secara bersamaan tetapi menggunakan skema yang berbeda. Skema yang ditemukan oleh Shamir dikenal dengan *threshold scheme* atau Shamir's *Secret Sharing Scheme*. Dalam *threshold scheme,* suatu *share* adalah suatu bagian dari informasi rahasia yang dimiliki oleh setiap anggota dalam suatu kelompok. Satu *(k,n)-threshold scheme* adalah suatu skema dimana setiap k anggota kelompok atau partisipan dari kelompok yang totalnya berjumlah n anggota, dapat menyusun kembali data rahasia yang sudah didistribusikan. Selain skema *Shamir's Secret Sharing*,

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

ada beberapa konsep skema pembagian rahasia, diantaranya adalah *(d,k,n)-Ramp Scheme*, *Online Secret Sharing*, *Graphical Secret Sharing*, *Non Graphical Secret Sharing*, dan sebagainya.

1.2 Permasalahan

Dalam skema pembagian rahasia dengan struktur akses *graphical*, yaitu skema pembagian rahasia yang berbasis graf, setiap simpul dapat dilihat sebagai suatu partisipan, setiap busur yang menghubungkan dua partisipan dapat dijadikan sebagai dasar skema pembagian rahasia, dimana pasangan partisipanyang mempunyai busur dapat merekonstruksi kunci rahasia K atau bisa juga sebaliknya, yaitu pasangan partisipan yang dihubungkan oleh busur tidak dapat merekonstruksi kunci rahasia K.

Dalam tulisan ini akan difokuskan pada masalah skema pembagian rahasia *non graphical* yang berdasarkan hipergraf. Permasalahan yang akan dibahas adalah bagaimanakah perbandingan antara skema pembagian rahasia yang berdasarkan struktur akses Γ dengan skema pembagian rahasia berdasarkan struktur terlarang Δ.

1.3 Tujuan Penulisan

Tujuan dari penelitian skema pembagian rahasia *non graphical* ini, adalah untuk:

1) Membandingkan skema pembagian rahasia yang berdasarkan struktur akses Γ dengan skema pembagian rahasia yang berdasarkan struktur terlarang Δ.
2) Menentukan *information rate* dari konstruksi pembagian rahasia yang dikaji.

1.4 Batasan Masalah

Masalah yang dibahas dalam penulisan ini akan dibatasi pada skema pembagian rahasia *non graphical* yang berdasarkan hipergraf dengan *rank* $r = 3$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

1.5 Sistematika Penulisan

Tesis ini akan disusun dalam lima bab dengan sistematika penulisan sebagai berikut:

BAB 1 : PENDAHULUAN

Menjelaskan latar belakang dilakukannya penelitian, permasalahan, tujuan penulisan, batasan masalah dan sistematika penulisan.

BAB 2 : LANDASAN TEORI

Berisikan tentang teori yang berkaitan dengan skema pembagian rahasia, mulai dari pengertian skema pembagian rahasia, struktur akses, *threshold scheme*, *information rate*, teori graf termasuk pengertian tentang hipergraf, serta o*ne-way hash function*.

BAB 3 : SKEMA PEMBAGIAN RAHASIA 3-STRUKTUR AKSES HIPERGRAF

Bab ini menjelaskan tentang skema pembagian rahasia *non-graphical* yang berdasarkan hipergraf *3-uniform* dengan struktur akses Γ, disebut sebagai skema 3-Struktur Akses Hipergraf (skema *3-SAH*), mulai dari konstruksi, rekonstruksi, sampai *information rate* dari skemanya.

BAB 4 : SKEMA PEMBAGIAN RAHASIA 3-STRUKTUR TERLARANG HIPERGRAF

Bab ini menjelaskan tentang skema pembagian rahasia *non-graphical* yang berbasis hipergraf *3-uniform* dengan struktur terlarang Δ, disebut sebagai skema 3-Struktur Terlarang Hipergraf (skema *3-STH*), mulai dari konstruksi, rekonstruksi, sampai *information rate* dari skemanya.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

BAB 5 : ANALISIS PERBANDINGAN SKEMA *3-SAH* DENGAN *3-STH*

Pada bab ini akan dibahas mengenai analisis perbandingan antara skema pembagian rahasia yang berdasarkan struktur akses Γ (skema *3-SAH*) dengan skema pembagian rahasia yang berdasarkan struktur terlarang Δ (skema *3-STH*) yang telah dibahas pada Bab 3 dan Bab 4.

BAB 6 : PENUTUP

Berisikan simpulan yang diperoleh dari hasil penelitian yang telah dilakukan serta saran yang dapat diberikan atas hasil penelitian.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

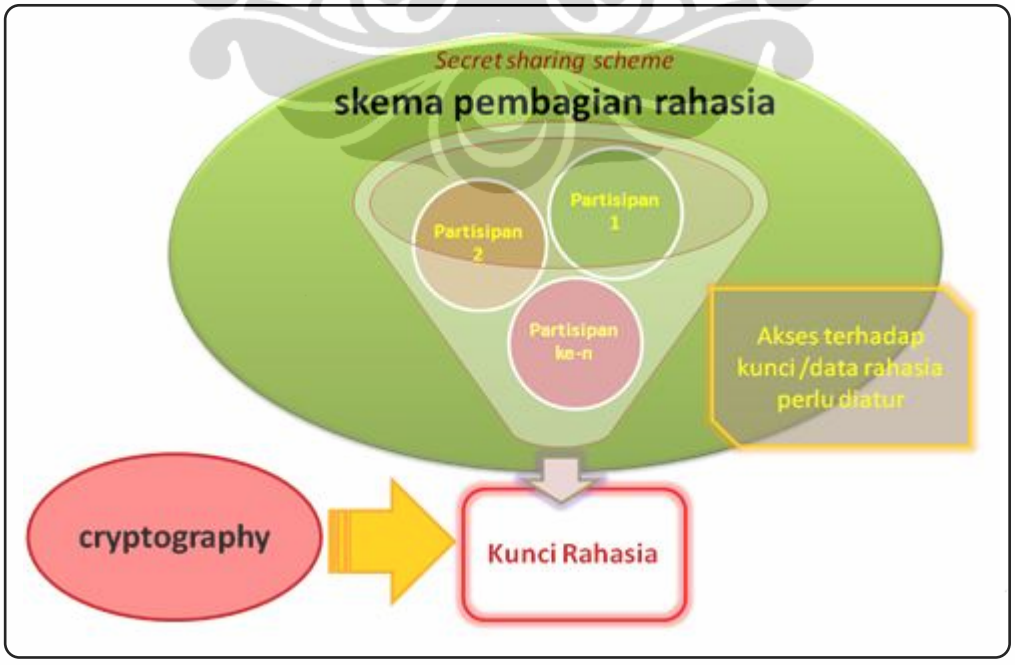
BAB 2
LANDASAN TEORI

Bab 2 berikut ini akan dibahas tentang landasan teori yaitu teori-teori yang berkaitan dengan skema pembagian rahasia, mulai dari pengertian, struktur akses, *threshold scheme*, *information rate*, teori graf termasuk pengertian tentang hipergraf, serta o*ne-way hash function*.

2.1 Skema Pembagian Rahasia

2.1.1 Pengertian

Dalam kritografi, proses penyandian data (*enkripsi*) dan membuka sandi (*dekripsi*) pasti menggunakan kunci penyandian. Kunci penyandian merupakan data rahasia yang sangat penting dan perlu dijaga supaya tidak jatuh pada pihak yang tidak berkepentingan. Artinya tidak semua orang boleh atau mempunyai akses terhadap data rahasia, sehingga perlu diatur siapa saja yang boleh mengakses data rahasia dan siapa yang tidak boleh. Salah satu metode yang digunakan untuk mengatur akses terhadap data/kunci rahasia adalah skema pembagian rahasia atau *secret sharing scheme*, seperti diilustrasikan pada Gambar 2.1.

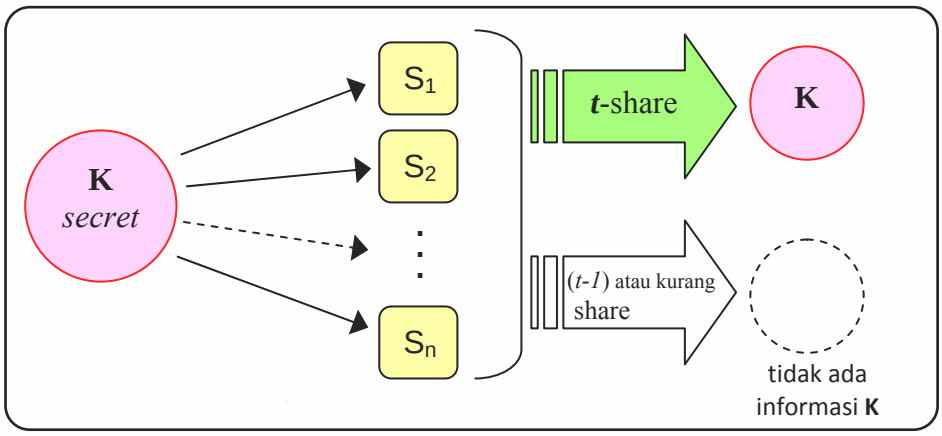


Gambar 2.1
Ilustrasi Pengaturan Akses terhadap Kunci Rahasia

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

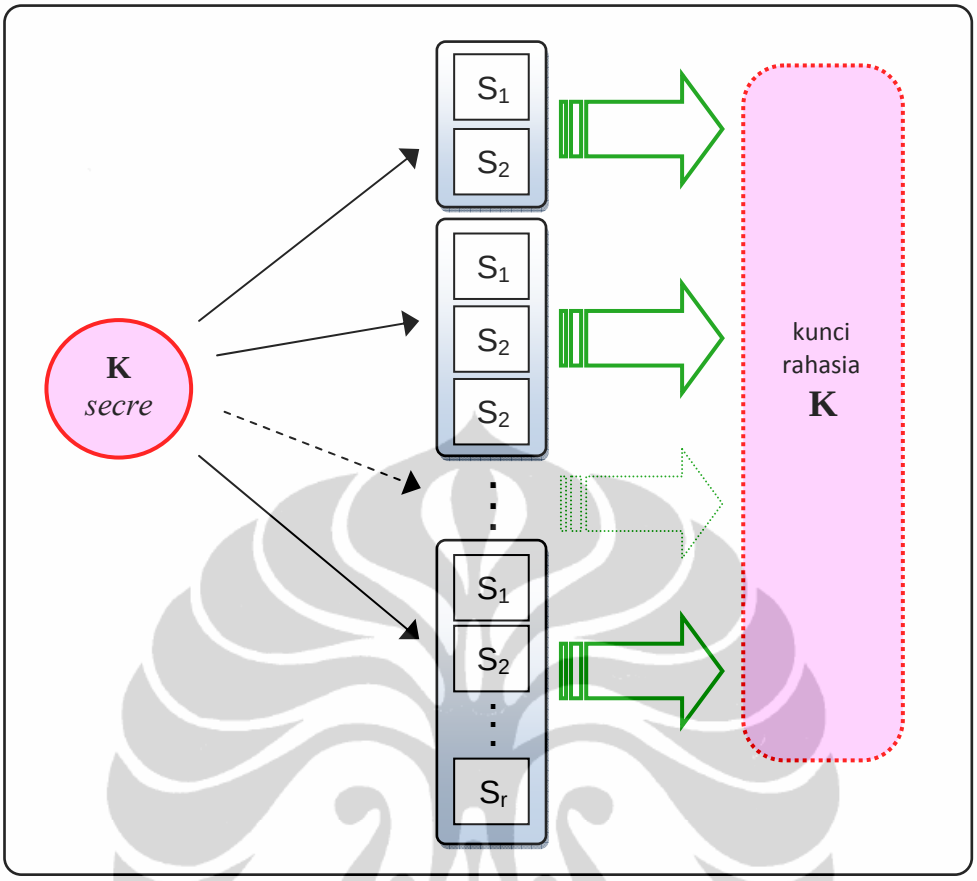
Pembagian (*sharing*) master kunci untuk mengakses informasi rahasia perlu diatur agar pihak yang tidak berkompeten tidak dapat mengakses informasi rahasia. Skema pembagian rahasia merupakan suatu skema dimana hanya sekelompok partisipan dengan kualifikasi tertentu saja yang dapat merekonstruksi informasi rahasia. Dalam skema pembagian rahasia, akses terhadap informasi rahasia yang diberikan kepada beberapa orang dengan kualifikasi tertentu disebut sebagai struktur akses. Misalnya terdapat partisipan sebanyak n orang, maka dalam merekonstruksi suatu data rahasia dibutuhkan t orang diantara n orang tersebut. Apabila kurang dari t maka data rahasia tidak bisa direkonstruksi. Skema pembagian rahasia pertama kali diperkenalkan oleh A. Shamir dan G. Blackley pada tahun 1979 secara bersamaan, dikenal dengan *threshold scheme* atau Shamir's *Secret Sharing Scheme* yang dinotasikan dengan *(t,n)-threshold scheme* (Shamir, 1979).

Dalam skema pembagian rahasia, *dealer* D akan membagi informasi rahasia yang dinotasikan dengan K kepada himpunan partisipan $P = \{p_1, p_2, ..., p_n\}$. Informasi rahasia yang dibagikan kepada himpunan P disebut dengan *share*, dinotasikan dengan S yang merupakan himpunan dari elemen-elemen S_i. Elemen S_i disebut dengan *share* ke-i untuk partisipan p_i, dengan $i = 1, 2, ..., n$. *Dealer* D merupakan partisipan khusus, dengan asumsi D bukan elemen dari P, yang bertanggung jawab untuk mengatur perhitungan dan distribusi dari *share*. Ilustrasi dari skema pembagian rahasia (t,n) - *threshold scheme* dapat dilihat pada Gambar 2.2.



Gambar 2.2
Skema Pembagian Rahasia (t,n) - *threshold scheme*

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.



Gambar 2.3
Skema Pembagian Rahasia *non-threshold scheme*

Berbeda dengan skema pembagian rahasia *threshold scheme*, skema pembagian rahasia yang bukan *threshold* dalam merekonstruksi suatu data rahasia tidak harus dibutuhkan *t* orang diantara *n* orang. Bisa saja lebih dari *t* orang atau kurang yang dapat merekonstruksi data rahasia. Ilustrasi skema pembagian rahasia yang bukan *threshold* dapat dilihat pada Gambar 2.2.

Berdasarkan sifatnya, skema pembagian rahasia dapat dibedakan menjadi skema pembagian rahasia *perfect* dan *nonperfect*. Suatu skema pembagian rahasia dikatakan *perfect* jika bagian dari partisipan yang tidak mempunyai kualifikasi tidak mempunyai informasi apapun mengenai rahasia *K*. Sebaliknya apabila tidak memenuhi persyaratan tersebut, maka skema pembagian rahasia dikatakan *nonperfect*.

Hal terpenting yang harus diperhatikan dalam implementasi skema pembagian rahasia adalah ukuran atau besarnya *share* yang dimiliki oleh

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

partisipan, karena keamanan dari skema pembagian rahasia akan berkurang jika ukuran / besarnya *share* bertambah. 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. Jika dalam rangkaian biner, *share* S_i mempunyai ukuran $\log_2|S_i|$ dan ukuran dari rahasia K adalah $\log_2|K|$, maka skema pembagian rahasia *perfect* akan memenuhi:

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

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

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

Ada beberapa pendekatan untuk mengkonstruksi suatu skema pembagian rahasia, antara lain polinomial, geometri, matroid, serta graf. Skema pembagain rahasia yang dapat direpresentasikan dengan graf disebut sebagai skema pembagian rahasia *graphical*. Skema pembagian rahasia yang dalam proses konstruksinya menggunakan struktur graf dapat diperluas dengan menggunakan hipergraf. Hipergraf merupakan bentuk yang lebih umum dari graf. Skema yang direpresentasikan dengan hipergraf merupakan salah satu bentuk dari skema pembagian rahasia *non-graphical*. Berbeda dengan skema pembagian rahasia *graphical* yang bisa digambarkan dalam dalam bentuk graf, skema pembagian rahasia *non-graphical* sangat sulit untuk digambarkan secara grafis. Dalam tesis ini yang akan dibahas adalah skema pembagian rahasia *non-graphical* yang berdasarkan hipergraf.

2.1.2 Struktur Akses

Struktur akses adalah kumpulan semua subset dari partisipan P dengan kualifikasi tertentu yang dapat menyusun atau merekonstruksi kunci rahasia. Itoh et al. (1987) menunjukkan bahwa suatu skema pembagian rahasia dikatakan *perfect* jika dan hanya jika struktur aksesnya monoton.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Struktur akses dinotasikan dengan Γ. Famili dari struktur akses Γ dikatakan monoton jika memenuhi:

$$A \in \Gamma, A \subseteq A' \subseteq P \Rightarrow A' \in \Gamma$$

Subset minimal dari Γ yang memenuhi $B \in \Gamma \ni B' \notin \Gamma \ \forall B' \subset B, B' \neq B$ disebut sebagai struktur akses minimal yang dinotasikan dengan Γ_0. Misalkan 2^P menunjukkan koleksi dari semua subset *P*, maka untuk setiap $\Gamma_0 \subseteq 2^P$ himpunan tertutup dari Γ_0 dinyatakan dengan:

$$cl(\Gamma_0) = \{A' : \exists A \in \Gamma_0, A \subseteq A' \subseteq P\}$$

Dalam skema pembagian rahasia *graphical* dan *non-graphical* terdapat tiga tipe struktur akses (Sun & Shieh, 1997), yaitu:

a) Tipe I: struktur akses Γ

   Untuk setiap skema pembagian rahasia dengan suatu struktur akses Γ dalam tipe I, hanya sub himpunan partisipan dalam struktur akses Γ yang dapat merekonstruksi kunci rahasia *K*, sedangkan yang lainnya tidak dapat merekonstruksi kunci rahasia *K*. Sebagai akibatnya, struktur terlarangnya adalah $\Delta = 2^P \setminus \Gamma$.

b) Tipe II: struktur terlarang Δ

   Untuk setiap skema pembagian rahasia dengan suatu struktur terlarang Δ dalam tipe II, hanya sub himpunan partisipan dalam struktur terlarang (*prohibited*) Δ yang tidak dapat merekonstruksi kunci rahasia *K*, sedangkan lainnya dapat merekonstruksi kunci rahasia *K*. Akibatnya struktur akses-nya adalah $\Gamma = 2^P \setminus \Delta$.

c) Tipe III: struktur campuran (Γ, Δ)

   Untuk setiap skema pembagian rahasia dengan suatu struktur campuran (Γ,Δ) dalam tipe III, sub himpunan partisipan dalam struktur akses Γ dapat merekonstruksi kunci rahasia *K* tetapi sub himpunan partisipan dalam struktur terlarang Δ tidak dapat merekonstruksi kunci rahasia *K*. Akibatnya adalah $\Gamma \cap \Delta = \phi$. Sub himpunan lain diluar dari Γ dan Δ yaitu $2^P \setminus (\Gamma \cup \Delta)$ tidak diperhatikan, artinya setiap sub

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

himpunan $2^P \setminus (\Gamma \cup \Delta)$ kemungkinan dapat merekonstruksi kunci rahasia K tetapi bisa juga tidak dapat merekonstruksi rahasia K. Himpunan $2^P \setminus (\Gamma \cup \Delta)$ bisa saja merupakan himpunan kosong.

Untuk setiap subset yang mempunyai kualifikasi $A \in \Gamma$, setiap superset dari A juga merupakan subset yang mempunyai kualifikasi secara intuitif. Hal ini menyebabkan suatu struktur akses Γ mempunyai sifat monoton naik, yaitu:

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

Dengan cara yang sama, untuk setiap subset yang tidak mempunyai kualifkasi $A \in \Delta$, setiap subset dari A juga merupakan suatu subset yang mempunyai kualifikasi. Sehingga struktur terlarang Δ mempunyai sifat monoton turun, yaitu:

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

2.1.3 *Threshold Scheme*

Dalam *threshold scheme* (Shamir, 1979), suatu *share* adalah suatu bagian dari informasi rahasia yang dimiliki oleh setiap anggota dalam suatu kelompok. Suatu *(t,n)-threshold scheme* adalah suatu skema dimana setiap *t* anggota kelompok (partisipan) dari kelompok yang totalnya berjumlah *n* anggota, dapat menyusun kembali informasi rahasia yang sudah didistribusikan.

Threshold Scheme diperkenalkan oleh A. Shamir dan G. Blackley pada tahun 1979. Dalam Shamir's *(t,n)-threshold scheme*, setiap *t* partisipan dapat merekonstruksi informasi rahasia *K*, tetapi setiap himpunan dengan partisipan yang kurang dari *t* tidak dapat merekonstruksi informasi rahasia *K*. Struktur akses dari *Shamir's (t,n)-threshold scheme*, adalah:

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

Sedangkan struktur terlarangnya adalah:

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

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Konstruksi skema Shamir's *(t,n)-threshold* didasarkan pada interpolasi polinomial. Agar *t-share* dari n partisipan dapat merekonstruksi informasi rahasia yang diberikan, maka dikonstruksi polinomial berderajat $(t-1)$ atas lapangan 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 lapangan 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 $K = 1234$ atas *field* Z_{7789}. Informasi rahasia K ini akan didistribusikan menjadi 6 bagian, dimana 3 *share*-nya akan dapat digunakan untuk merekonstruksi K. Sehingga diperoleh $n = 6$ dan $t = 3$. Karena $t = 3$, maka persamaan polinomial 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:

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

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*.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

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:

$$(x_0, y_0) = (1,1494);$$
$$(x_1, y_1) = (2,1942);$$
$$(x_2, y_2) = (3,2578).$$

Untuk merekonstruksi polinom digunakan interpolasi Lagrange, yaitu:

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

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

$$l_1(x) = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-1}{2-1} \cdot \frac{x-3}{2-3}$$
$$= \frac{(x-1)(x-3)}{(-1)} = -\left(x^2 - 4x + 3\right)$$

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

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

$$= 1494\left(\frac{1}{2}\left(x^2 - 5x + 6\right)\right) + 1942\left(-x^2 + 4x - 3\right)$$
$$+ 2578\left(\frac{1}{2}\left(x^2 - 3x + 2\right)\right)$$

$$= (747 - 1942 + 1289)x^2 + (-3735 + 7768 - 3867)x$$
$$+ (4482 - 5826 + 2578)$$

$$= 94x^2 + 166x + 1234$$

Sehingga diperoleh $K = a_0 = 1234$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

2.1.4 *Information Rate*

Tingkat efisiensi dari skema pembagian rahasia dapat diukur dari rata-rata informasinya yaitu perbandingan antara ukuran kunci rahasia dengan ukuran *share* yang terbesar, atau dikenal dengan *information rate* yang dinotasikan dengan ρ. Misalkan $P = \{p_1, p_2, ..., p_n\}$ adalah himpunan dari semua partisipan dengan 2^P adalah kumpulan dari semua subhimpunan *P*. Misalkan *K* menunjukkan informasi rahasia yang didistribusikan kepada 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 $\log_2 |S|$. *Information rate* dari skema pembagian rahasia Brickell dan Davenport (1991) dinyatakan dengan:

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

Dalam implementasi skema pembagian rahasia, sangat penting untuk meminimalkan besarnya / ukuran *share* yang didistribusikan kepada setiap partisipan. Dengan kata lain *information rate* yang diinginkan adalah sebesar mungkin. *Information rate* dari skema pembagian rahasia yang *perfect* akan selalu mempunyai nilai antara nol sampai dengan satu (Capocelli et al. 1993 dan Csirmaz, 1997). Suatu skema pembagian rahasia dikatakan ideal jika $\rho = 1$.

Information rate dari skema pembagian rahasia yang dirumuskan oleh Brickell dan Davenport (1991) bisa dilihat dari struktur suatu hipergraf. Skema pembagian rahasia yang struktur aksesnya berdasarkan hipergraf dapat dilihat dari struktur akses Γ maupun dari sisi struktur terlarang Δ. Wang dan Juan (2007) merumuskan *information rate* ρ pada stuktur hipergraf *H 3-uniform* dengan stuktur akses Γ. Misalkan banyaknya simpul-simpul dari suatu hipergraf *H 3-uniform* adalah *n*, sedangkan d_{max} menunjukkan derajat maksimum dari hipergraf *H*. Maka *information*

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

rate ρ dari suatu skema pembagian rahasia dengan struktur akses Γ yang berdasarkan hipergraf H *3-uniform* akan memenuhi:

$$\rho = \frac{2}{\left(d_{\max} + 1\right)}$$

Sedangkan *Information rate* dari suatu skema pembagian rahasia dengan struktur terlarang Δ yang berdasarkan suatu hipergraf H *r-uniform* menurut Weng dan Juan (2005) akan memenuhi:

$$\rho = \max\left\{3/(C(n-1,r-1) - d_{\min} + r + 1), 3/(C(n-1,r-1) + 1)\right\}$$

dimana d_{min} merupakan derajat minimum dari hipergraf H sedangkan n adalah banyaknya simpul-simpul dari H.

2.2 Teori Graf

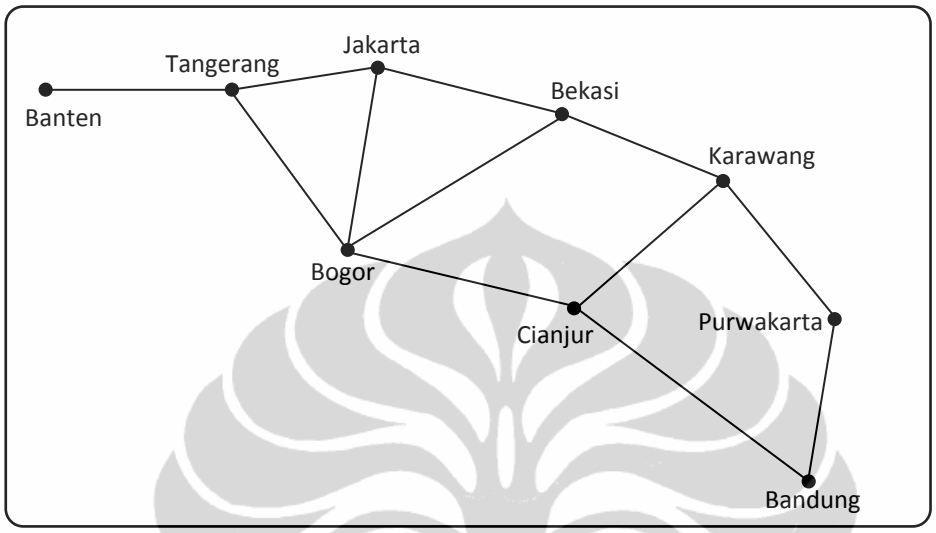
2.2.1 Graf

Graf merupakan suatu konsep yang menggambarkan struktur diskrit yang terdiri atas simpul-simpul (*vertices*) dan busur-busur (*edges*) yang menghubungkan simpul-simpul. Teori Graf pertama kali diperkenalkan oleh ahli matematika Swiss, Leonhard Euler, pada tahun 1736 (Garnier & Taylor, 2002). Euler menggunakan konsep graf untuk memecahkan persolan jembatan Königsberg. Saat ini konsep graf banyak dipergunakan untuk memecahkan persoalan pada berbagai aplikasi diantaranya pada rangkaian elektronik, ikatan isomer kimia, jaringan komputer (*computer network*), jaringan transportasi, dan sebagainya.

Graf sederhana $G = (V, E)$ terdiri dari V dan E, dimana V merupakan himpunan tak kosong dari simpul-simpul, sedangkan E adalah himpunan tak berurut pasangan elemen-elemen dari V yang disebut busur. Graf sederhana merupakan graf yang tidak berarah dan tidak memiliki busur ganda maupun *loop*. Busur ganda merupakan suatu busur yang menghubungkan dua buah simpul yang sama. Sedangkan *loop* merupakan suatu busur yang mempunyai awal dan akhir pada simpul yang sama. Graf yang diaplikasikan dalam skema pembagian rahasia dengan struktur akses berdasarkan graf adalah graf sederhana. Salah satu contoh dari graf sederhana adalah peta

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

jalan yang menghubungkan beberapa kota dari Banten, Jakarta sampai Bandung, seperti ditunjukkan pada Gambar 2.4.



Gambar 2.4:
Graf Sederhana

2.2.2 Hipergraf

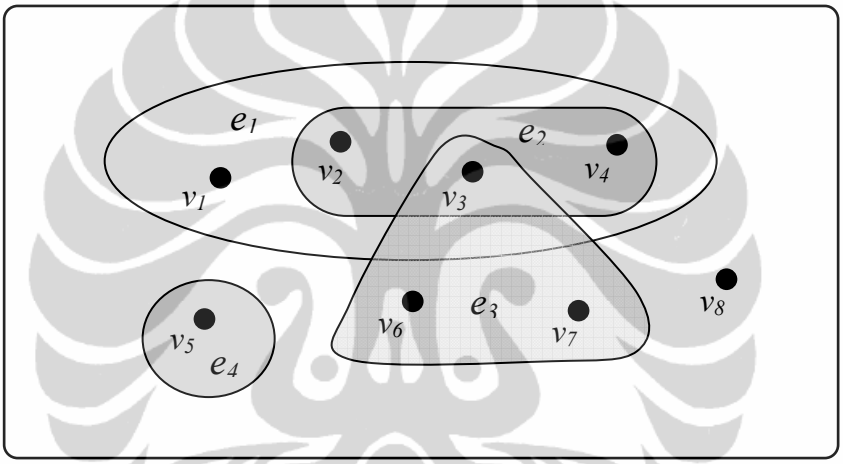
Dalam teori graf, suatu busur dari graf sederhana dapat menghubungkan dua buah simpul. Berbeda dengan graf, dalam teori hipergraf suatu busur dapat dipandang sebagai suatu subset sembarang dari simpul-simpul. Hipergraf merupakan generalisasi dari graf.

Suatu hipergraf $H = (V, E)$ adalah suatu himpunan berhingga V simpul-simpul bersama dengan suatu himpunan berhingga E busur-busur (disebut sebagai hiperbusur) yang merupakan subset sembarang dari V. Derajat hiperbusur dari suatu hipergraf ditunjukkan oleh kardinalitas hiperbusur (Rosen, 2000).

Jadi suatu hipergraf H merupakan pasangan terurut (V,E), dimana V adalah himpunan tak nol dari simpul-simpul, sedangkan hiperbusur dapat dituliskan $E = \{E_1, E_2, ..., E_m\} \subseteq 2^V$ dengan $|E_i| \geq 2$ untuk $1 \leq i \leq m$. Derajat dari suatu simpul u adalah $|\{E_i : u \in E_i \text{ untuk } 1 \leq i \leq m\}|$, yang besarnya

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

dituliskan dengan *d(H)*. Jika $|E_i| = r \geq 2$ untuk semua $1 \leq i \leq |E|$ maka hipergraf *H* disebut sebagai hipergraf *r-uniform*, dengan kata lain hipergraf adalah *uniform* jika semua hiperbusur dari suatu hipergraf mempunyai jumlah simpul yang sama. Graf merupakan suatu hipergraf *2-uniform*. Suatu hipergraf dikatakan regular jika semua simpul-simpulnya mempunyai derajat yang sama. Tidak seperti graf, hipergraf sangat sulit untuk digambar sehingga cenderung digambarkan dengan menggunakan teori himpunan. Ilustrasi dari suatu hipergraf dapat dilihat pada Gambar 2.4.



Gambar 2.5: Hipergraf

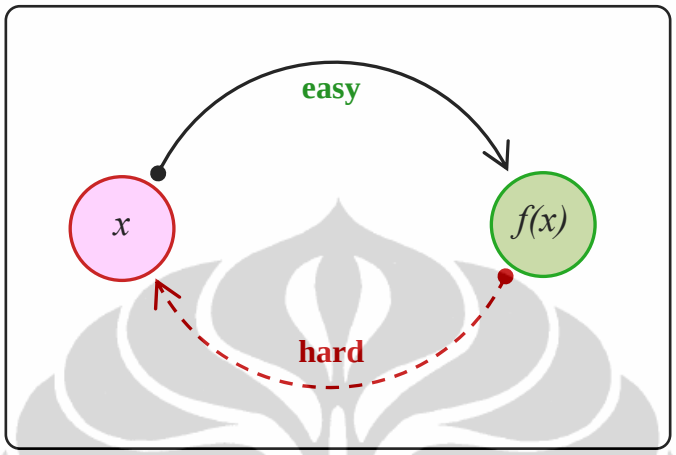
Dari Gambar 2.4 dapat dilihat suatu hipergraf $H = (V, E)$ dengan $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8\}$ dan $E = \{e_1, e_2, e_3, e_4\} = \{\{v_1, v_2, v_3, v_4\}, \{v_2, v_3, v_4\}, \{v_3, v_6, v_7\}, \{v_5\}\}$.

2.3 *One Way Hash Function*

Fungsi *hash* telah banyak digunakan dalam ilmu komputer (*computer science*). Fungsi *hash* adalah suatu fungsi yang mengambil suatu input *binary string* dengan panjang berubah-ubah (disebut dengan *pre-image*) dan mengubahnya menjadi *binary string* dengan panjang tetap (disebut dengan *hash value*) (Schneier, 1986). Sedangkan *one-way function* merupakan suatu fungsi satu arah yang relatif mudah untuk dihitung tetapi sulit untuk mencari

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

inverse-nya, seperti ilustrasi pada Gambar 2.5. Jika diberikan x maka sangat mudah untuk menghitung fungsi $f(x)$, tetapi jika diberikan $f(x)$ maka akan sangat sulit untuk menghitung x.



Gambar 2.6 :
Ilustrasi *One Way Function* [Sumber: Goldreich, 2004, p.31]

One way hash function mempunyai banyak nama diantaranya adalah *compression function*, *contraction function*, *message digest*, *fingerprint*, *cryptographic checksum*, *message integrity check* (*MIC*), dan *manipulation detection code* (*MDC*).

Suatu *one-way hash function H(M)*, beroperasi pada suatu *pre-image message M* dengan panjang sembarang, menghasilkan suatu nilai *hash h* dengan panjang tetap.

$h = H(M)$, dengan h panjangnya m

One way hash function mempunyai karakteristik:

a) Jika diberikan M, maka mudah untuk menghitung h.
b) Jika diberikan h, maka akan sulit untuk menghitung M sedemikian sehingga $H(M) = h$.
c) Jika diberikan M, maka akan sulit untuk menentukan *message* yang lain M', sedemikian sehingga $H(M) = H(M')$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Salah satu contoh sederhana dari *one way hash function* adalah operasi *x-or*, yang merupakan suatu fungsi yang mengambil *pre-image* dengan mengoperasikan *x-or* semua *byte-byte* input dan mengembalikan menjadi suatu *byte* (Stallings, 2003).

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

BAB 3
SKEMA PEMBAGIAN RAHASIA 3-STRUKTUR AKSES HIPERGRAF

Dalam konstruksi skema pembagian rahasia berdasarkan hipergraf, setiap simpul pada hipergraf dapat dilihat sebagai suatu partisipan dalam skema pembagian rahasia. Seperti telah dijelaskan pada Bab 2 tentang struktur akses skema pembagian rahasia menurut Sun dan Shieh (1997), untuk struktur tipe I dalam skema pembagian rahasia yang berdasarkan hipergraf, struktur akses Γ adalah himpunan partisipan yang bersesuaian dengan hiperbusur. Artinya hanya partisipan yang bersesuaian dengan hiperbusur yang dapat merekonstruksi kunci rahasia *K*. Untuk struktur campuran (Γ,Δ) dalam tipe III, struktur Γ terdiri dari partisipan-partisipan yang bersesuaian dengan hiperbusur dari hipergraf dapat merekonstruksi kunci rahasia *K*, sedangkan Δ terdiri dari partisipan-partisipan yang tidak dihubungkan oleh hiperbusur tidak dapat merekonstruksi kunci rahasia *K*. Untuk struktur terlarang Δ (tipe II) dalam skema pembagian rahasia berdasarkan hipergraf, struktur Γ adalah $\Gamma = 2^P \setminus \Delta$ dimana P menunjukkan himpunan partisipan, sedangkan Δ merupakan himpunan partisipan yang tidak bersesuaian dengan hiperbusur. Dalam bab ini akan dibahas mengenai skema pembagian rahasia tipe I yang berdasarkan hipergraf *3-uniform*, yaitu skema pembagian rahasia 3-Struktur Akses Hipergraf atau disingkat dengan skema *3-SAH*. Konstruksi skema *3-SAH* yang dijelaskan dalam Bab 3 ini diambil dari paper Wang dan Juan (2007).

3.1 Konstruksi Skema *3-SAH*

Misalkan $H = (P, S)$ suatu hipergraf dimana $P = \{p_1, p_2, ..., p_n\}$ merupakan himpunan partisipan dari skema pembagian rahasia yang masing-masing partisipan direpresentasikan sebagai simpul-simpul suatu hipergraf *H* sedangkan *S* merupakan himpunan *r*-partisipan yang bersesuaian dengan hiperbusur dalam *H*. Dalam konstruksi skema *3-SAH*, hiperbusur yang terbentuk terdiri dari 3 simpul. Himpunan dari *3* partisipan yang bersesuaian dengan hiperbusur adalah subhimpunan dari partisipan yang merupakan *share*

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

dari skema *3-SAH*, dinyatakan dengan $S = \{A : A \in E(H)\}$. Kumpulan semua subset *P* yang dapat menyusun atau merekonstruksi kunci rahasia *K* disebut sebagai struktur akses Γ. Struktur akses dalam skema *3-SAH* menggunakan struktur akses tipe I. Struktur akses Γ disusun berdasarkan partisipan yang bersesuaian dengan hiperbusur dari hipergraf *H*, dinyatakan dengan $\Gamma = \{A \subseteq P \mid S \subseteq A \text{ untuk setiap } S \subseteq \Gamma_0\}$. Sedangkan struktur akses minimal Γ_0 merupakan suatu famili dari himpunan minimal dalam Γ (subset minimal dari Γ), dinyatakan dengan $\Gamma_0 = \{A \in \Gamma : A' \not\subset A \ \forall A' \in \Gamma - \{A\}\}$. Sesuai dengan struktur askes tipe I, maka struktur terlarang dari skema *3-SAH* dinyatakan dengan $\Delta = 2^P \setminus \Gamma = \{A \subseteq P \mid S \not\subset A \ \forall S \subseteq \Gamma_0\}$.

Kunci rahasia *K* dari skema *3-SAH* dinyatakan dengan $K = \{K_0, K_1\}$, dimana K_0 dan K_1 diambil secara acak dari bilangan Z_q dengan *q* merupakan bilangan prima. Dalam menentukan *share* dari partisipan dalam konstruksi skema *3-SAH* digunakan suatu fungsi satu arah *hash* (g_{hash}). Dalam Tesis ini akan digunakan fungsi *hash* sederhana yaitu operasi *x-or*. Semua perhitungan dalam konstruksi skema *3-SAH* adalah atas lapangan Z_q, dengan $q > \max\{K_0, K_1\}$ adalah bilangan prima yang besar.

Berikut adalah langkah-langkah konstruksi pembentukan skema pembagian rahasia *3-SAH*.

Langkah 1: Pilih kunci rahasia $K = \{K_0, K_1\}$ dimana K_0 dan K_1 diambil secara acak dari bilangan Z_q sedangkan k_2 diambil acak dari Z_q.

Langkah 2: *Dealer D* mengkonstruksi fungsi polinomial

$$f(x) = k_2 x^2 + K_1 x + K_0 .$$

Langkah 3: Hitung $y_{(i_1,i_2)} = f\left(\sum_{k=1}^{2} i_k n^{3-k-1}\right)$ untuk $1 \le i_1 < i_2 \le n$.

Langkah 4: Pilih *n* bilangan acak $a_1, a_2, ..., a_n$ dari Z_q.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Langkah 5: Untuk $1 \le i \le n$, tentukan *share*

$$S_i = \left\langle a_{i,(1,2)},...,a_{i,(j_1,j_2)},...,a_{i,(n-1,n)},a_i \right\rangle \text{ untuk } 1 \le j_1 < j_2 \le n,$$

dimana:

$$a_{i,(j_1,j_2)} = \begin{cases} y_{(j_1,j_2)} + g_{hash}(a_{j_1} \oplus a_{j_2}), \text{ jika } \{p_i, p_{j_1}, p_{j_2}\} \in E(G); \\ \text{kosong, untuk lainnya} \end{cases}$$

Langkah 6: Kirim *share* S_i ke partisipan p_i, untuk $i = 1,2,...,n$.

Share S_i untuk partisipan p_i, dengan $i = 1,2,...,7$ pada proses konstruksi skema *3-SAH* secara umum untuk hipergraf Gambar 3.1 dapat dilihat pada Tabel 3.1. Tanda "-" dalam tabel menunjukkan bahwa *subshare*-nya kosong. Konstruksi skema *3-SAH* akan memenuhi kondisi sebagai berikut:

(1) jika $A \subseteq P$ dan $|A| < 3$, maka *A* tidak akan mempunyai informasi rahasia.

(2) jika $e \not\subset A \subseteq P \forall e \in \Gamma_0$ dan $|A| \ge 3$, maka *A* tidak akan mempunyai informasi rahasia.

(3) jika $\exists e \in \Gamma_0, e \subseteq A \subseteq P$ dan $|A| \ge 3$, maka *A* dapat merekonstruksi kunci rahasia *K*.

Penjelasan mengenai ketiga kondisi tersebut akan dibahas pada bagian Analisis Keamanan Skema *3-SAH*.

3.2 Rekonstruksi Skema *3-SAH*

Dari konstruksi skema pembagian rahasia *3-SAH* akan diperoleh suatu *share* S_i dari partisipan p_i, untuk $i = 1,2,...,n$. Tabel *share* secara umum dari skema *3-SAH* untuk *n = 7* dapat dilihat pada Tabel 3.1. Dari skema *share* yang diperoleh dalam proses konstruksi skema *3-SAH*, dapat direkonstruksi untuk memperoleh struktur kunci rahasia *K*. Langkah-langkah proses rekonstruksi skema *3-SAH* adalah sebagai berikut:

Langkah 1: Ambil *share* $S_{j_1}, S_{j_2}, S_{j_3}$ dari partisipan $p_{j_1}, p_{j_2}, p_{j_3}$ untuk $1 \le j_1 < j_2 < j_3 \le n$, dimana $A = \{p_{j_1}, p_{j_2}, p_{j_3}\}$ adalah subset minimal dari *P* yang dapat menyusun atau merekonstruksi kunci rahasia *K*, dengan kata lain $A \subseteq \Gamma_0$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Langkah 2: Ambil $\{i_1, i_2\} = \{j_1, j_2, j_3\} \setminus \{t\}$, untuk $1 \le t \le 3$, kemudian dihitung $y_{(i_1,i_2)}$ dengan $y_{(i_1,i_2)} = a_{k,(i_1,i_2)} - g_{hash}(a_{i_1} \oplus a_{i_2})$.

Langkah 3: Koleksi 3 titik-titik $\left(\sum_{k=1}^{2} i_k n^{3-k-1}, y_{(i_1,i_2)}\right)$ dari langkah 2. Dengan bantuan *3* titik tersebut, polinomial $f(x) = k_2 x^2 + K_1 x + K_0$ dapat direkonstruksi menggunakan interpolasi Lagrange.

Langkah 4: Setelah polinomial $f(x) = k_2 x^2 + K_1 x + K_0$ direkonstruksi, maka informasi rahasia $K = \{K_0, K_1\}$ dapat diperoleh.

3.3 Analisis Keamanan Skema *3-SAH*

Konstruksi skema *3-SAH* akan memenuhi 3 kondisi yaitu jika $A \subseteq P$ dan $|A| < 3$, maka A tidak akan mempunyai informasi rahasia, jika $e \not\subset A \subseteq P \forall e \in \Gamma_0$ dan $|A| \ge 3$, maka A tidak akan mempunyai informasi rahasia, sedangkan jika $\exists e \in \Gamma_0, e \subseteq A \subseteq P$ dan $|A| \ge 3$, maka A dapat merekonstruksi kunci rahasia *K*. Berikut ini akan dijelaskan mengenai analisis keamanan serta analisis *information rate* dari skema *3-SAH*.

Teorema 3.1: Untuk semua $A \subseteq P$ dan $|A| < 3$, maka A tidak akan mempunyai informasi apapun tentang kunci rahasia *K* dari skema *3-SAH*.

Bukti:

Tanpa menghilangkan sifat umumnya, misalkan diambil $|A| = 2$ dan $A = \{p_{j_1}, p_{j_2}\}$, dengan $1 \le j_1 < j_2 \le n$. *Share* dari partisipan p_i untuk $i \in \{j_1, j_2\}$ adalah $S_i = \langle a_{i,(1,2)}, ..., a_{i,(j_1,j_2)}, ..., a_{i,(n-1,n)}, a_i \rangle$. Karena $A = \{p_{j_1}, p_{j_2}\}$ untuk semua $0 \le j_1 < j_2 \le n$, maka *share* dari p_{j_1} adalah $S_{j_1} = \langle a_{j_1,(1,2)}, ..., a_{j_1,(j_1,j_2)}, ..., a_{j_1,(n-1,n)}, a_{j_1} \rangle$, sedangkan *share* p_{j_2} adalah $S_{j_2} = \langle a_{j_2,(1,2)}, ..., a_{j_2,(j_1,j_2)}, ..., a_{j_2,(n-1,n)}, a_{j_2} \rangle$. Akibatnya tidak diperoleh

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

informasi tentang $y_{(j_1,j_2)}$ yang bisa diturunkan dari S_{j_1}, S_{j_2}. Karena $y_{(j_1,j_2)}$ tidak dapat diketahui maka partisipan p_{j_1}, p_{j_2} tidak dapat merekonstruksi kunci rahasia *K*. □

Teorema 3.2: Jika $e \not\subset A \subseteq P \ \forall e \in \Gamma_0$ dan $|A| \geq 3$, maka *A* tidak akan mempunyai informasi tentang kunci rahasia *K* dari skema *3-SAH*.

Bukti:

Misalkan $A = \{p_{m_1}, p_{m_2}, ..., p_{m_l}\}$, dimana $1 \leq m_1 < m_2 < ... < m_l \leq n$ dan $l \geq 3$. Misalkan $S_i = \langle a_{i,(1,2)}, ..., a_{i,(j_1,j_2)}, ..., a_{i,(n-1,n)}, a_i \rangle$ adalah kumpulan *share* dari partisipan p_i untuk $i \in \{m_1, m_2, ..., m_l\}$. Karena $e \not\subset A \subseteq P$ untuk semua $e \in \Gamma_0$, maka informasi tentang $y_{(j_1,j_2)}$ untuk setiap $1 \leq j_1 < j_2 \leq n$ tidak akan diperoleh dari *share* $S_{m_1}, S_{m_2}, ..., S_{m_l}$, serta tidak akan terpengaruh oleh $\{j_1, j_2\} \subseteq \{m_1, m_2, ..., m_l\}$ atau $\{j_1, j_2\} \not\subset \{m_1, m_2, ..., m_l\}$. Sehingga partisipan-partisipan $p_{m_1}, p_{m_2}, ..., p_{m_l}$ tidak dapat merekonstruksi kunci rahasia *K*. □

Teorema 3.3: Jika $\exists e \in \Gamma_0, e \subseteq A \subseteq P$ dan $|A| \geq 3$, maka *A* dapat merekonstruksi kunci rahasia *K*.

Bukti:

Misalkan $\{p_{m_1}, p_{m_2}, p_{m_3}\} = e \subseteq A$, untuk sembarang $e \in \Gamma_0$ dimana $1 \leq m_1 < m_2 < m_3 \leq n$. Misalkan kumpulan *share* dari partisipan p_i untuk $i \in \{m_1, m_2, m_3\}$ adalah $S_i = \langle a_{i,(1,2)}, ..., a_{i,(j_1,j_2)}, ..., a_{i,(n-1,n)}, a_i \rangle$. Berdasarkan langkah-langkah konstruksi skema *3-SAH*, maka akan diperoleh 3 *sub*kunci $y_{(j_1,j_2)}$ untuk $1 \leq j_1 < j_2 \leq n$ dan $\{j_1, j_2\} \subseteq \{m_1, m_2, m_3\}$. Sehingga partisipan-partisipan $p_{m_1}, p_{m_2}, p_{m_3}$ dapat merekonstruksi kunci rahasia *K*. □

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Teorema 3.4: Misalkan banyaknya simpul-simpul dari suatu hipergraf *H* *3-uniform* adalah *n*, sedangkan d_{max} menunjukkan derajat maksimum dari hipergraf *H*. Maka *information rate* ρ dari suatu skema *3-SAH* yang berdasarkan hipergraf *H* akan memenuhi:

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

Bukti:

Share S_i untuk partisipan p_i, untuk $i = 1, 2, ..., n$ merupakan suatu vektor dengan elemen $(C(n,2)+1)$, dimana $C(x,y) = x!/(y!(x-y)!)$. Untuk elemen pertama $C(n,2)$, jika $\{p_i, p_{l_1}, p_{l_2}, p_{l_3}\} \notin E(H)$ untuk $1 \le l_1 < l_2 < l_3 \le n$, maka $a_{i,(x_1,x_2)}$ kosong untuk $\{i, x_1, x_2\} = \{l_1, l_2, l_3\}$. Artinya $a_{i,(x_1,x_2)}$ adalah atas lapangan Z_q hanya jika $\{p_i, p_{x_1}, p_{x_2}\} \in E(H)$ untuk $1 \le x_1 < x_2 \le n$.

Untuk elemen terakhir, yaitu 1, a_i selalu ada (eksis). Sehingga *share* S_i akan sama dengan $\lceil Z_q \rceil^{\deg(p_i)+1}$, dimana $\deg(p_i)$ merupakan derajat dari simpul p_i dalam hipergraf *H*. Karena ruang *share* maksimal adalah $\lceil Z_q \rceil^{d+1}$ dimana *d* merupakan derajat maksimal dari hipergraf *H* dan kunci rahasia *K* memenuhi $K = \lceil Z_q \rceil^2$, maka *information rate* dari skema *3-SAH* akan memenuhi:

$$(2\log q)/((d+1)\log q) = 2/(d+1) \qquad \square$$

Untuk memberikan gambaran yang lebih jelas dalam pembentukan skema pembagian rahasia *3-SAH*, mulai dari proses konstruksi dan rekonstruksi dapat diperhatikan pada Contoh 3.5.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

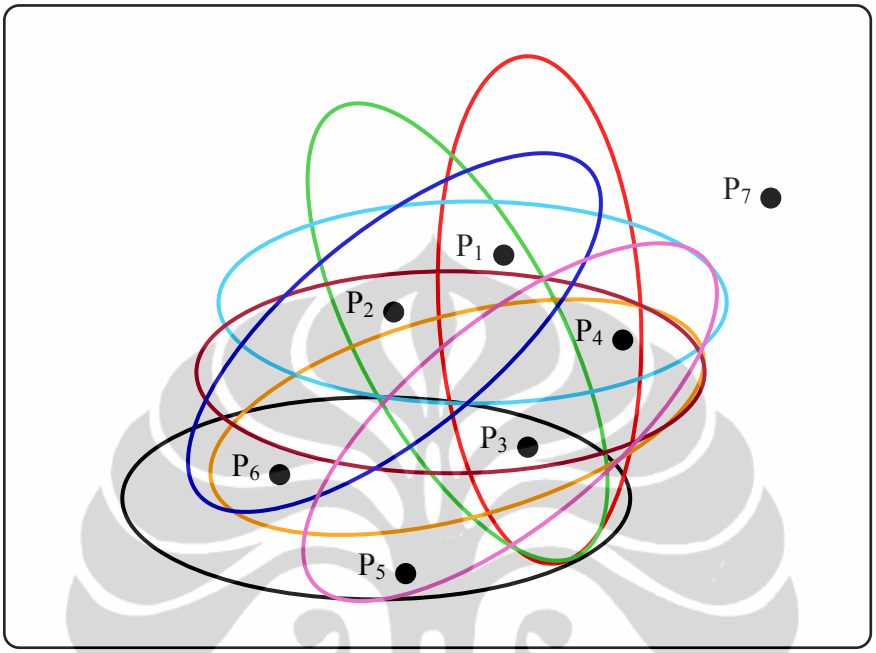
Tabel 3.1: *Share* Secara Umum dari Skema *3-SAH* untuk Hipergraf pada Gambar 3.1

	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$a_{i,(1,2)}$	-	-	$y_{(1,2)} + g_{hash}(r_1 \oplus r_2)$	$y_{(1,2)} + g_{hash}(r_1 \oplus r_2)$	-	$y_{(1,2)} + g_{hash}(r_1 \oplus r_2)$	-
$a_{i,(1,3)}$	-	$y_{(1,3)} + g_{hash}(r_1 \oplus r_3)$	-	$y_{(1,3)} + g_{hash}(r_1 \oplus r_3)$	-	-	-
$a_{i,(1,4)}$	-	$y_{(1,4)} + g_{hash}(r_1 \oplus r_4)$	$y_{(1,4)} + g_{hash}(r_1 \oplus r_4)$	-	-	-	-
$a_{i,(1,5)}$	-	-	-	-	-	-	-
$a_{i,(1,6)}$	-	$y_{(1,6)} + g_{hash}(r_1 \oplus r_6)$	-	-	-	-	-
$a_{i,(1,7)}$	-	-	-	-	-	-	-
$a_{i,(2,3)}$	$y_{(2,3)} + g_{hash}(r_2 \oplus r_3)$	-	-	$y_{(2,3)} + g_{hash}(r_2 \oplus r_3)$	-	-	-
$a_{i,(2,4)}$	$y_{(2,4)} + g_{hash}(r_2 \oplus r_4)$	-	$y_{(2,4)} + g_{hash}(r_2 \oplus r_4)$	-		-	
$a_{i,(2,5)}$	-	-	-	-	-	-	-
$a_{i,(2,6)}$	$y_{(2,6)} + g_{hash}(r_2 \oplus r_6)$	-	-	-	-	-	-
$a_{i,(2,7)}$	-	-	-	-	-	-	-
$a_{i,(3,4)}$	$y_{(3,4)} + g_{hash}(r_3 \oplus r_4)$	$y_{(3,4)} + g_{hash}(r_3 \oplus r_4)$	-	-	$y_{(3,4)} + g_{hash}(r_3 \oplus r_4)$	$y_{(3,4)} + g_{hash}(r_3 \oplus r_4)$	-
$a_{i,(3,5)}$	-	-	-	$y_{(3,5)} + g_{hash}(r_3 \oplus r_5)$	-	$y_{(3,5)} + g_{hash}(r_3 \oplus r_5)$	-
$a_{i,(3,6)}$	-	-	-	$y_{(3,6)} + g_{hash}(r_3 \oplus r_6)$	$y_{(3,6)} + g_{hash}(r_3 \oplus r_6)$	-	-
$a_{i,(3,7)}$	-	-	-	-	-	-	-
$a_{i,(4,5)}$	-	-	$y_{(4,5)} + g_{hash}(r_4 \oplus r_5)$	-	-	-	-
$a_{i,(4,6)}$	-	-	$y_{(4,6)} + g_{hash}(r_4 \oplus r_6)$	-	-	-	-
$a_{i,(4,7)}$	-	-	-	-	-	-	-
$a_{i,(5,6)}$	-	-	$y_{(5,6)} + g_{hash}(r_5 \oplus r_6)$	-	-	-	-
$a_{i,(5,7)}$	-	-	-	-	-	-	-
$a_{i,(6,7)}$	-	-	-	-	-	-	-
a_i	a_1	a_2	a_3	a_4	a_5	a_6	a_7

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Contoh 3.5:

Gambar 3.1 berikut ini menunjukkan suatu hipergraf *H* yang akan digunakan sebagai dasar dalam mengkonstruksi skema *3-SAH*.



Gambar 3.1
Contoh *3-Uniform* Hipergraf *H=(V,E)*

Dari Gambar 3.1 dapat diperoleh:

$$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$$

$$E(H) = \Gamma_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_2, p_6\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}, \{p_3, p_4, p_5\}, \{p_3, p_4, p_6\}, \{p_3, p_5, p_6\}\}$$

$$\Gamma = \{A \subseteq P \mid S \subseteq A \ \forall S \subseteq \Gamma_0\}$$

$$\Delta = 2^P \setminus \Gamma = \{A \subseteq P \mid S \not\subset A \ \forall S \subseteq \Gamma_0\}$$

Langkah-langkah konstruksi skema *3-SAH* berdasarkan Gambar 3.1 adalah sebagai berikut:

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Langkah 1: Misalkan rahasia $K = \{K_0, K_1\} = \{179, 241\}$ yang diambil secara acak dari Z_q dan $k_2 = 293$ diambil acak dari Z_{331}.

Langkah 2: *Dealer D* mengkonstruksi polinomial $f(x) = k_2 x^2 + K_1 x + K_0$, yaitu $f(x) = 293x^2 + 241x + 179$.

Langkah 3: Hitung $y_{(i_1,i_2)} = f\left(\sum_{k=1}^{2} i_k n^{3-k-1}\right)$ untuk $1 \le i_1 < i_2 \le n$.

Langkah 4: Pilih *7* bilangan acak $a_1, a_2, ..., a_7$ dari Z_{331} yaitu:

$a_1 = 31,\ a_2 = 45,\ a_3 = 57,\ a_4 = 63,\ a_5 = 70,\ a_6 = 82,\ a_7 = 96$

Langkah 5: Fungsi *hash* yang digunakan pada contoh ini adalah fungsi *has*h sederhana *x-or* p_i (yang dinotasikan dengan $\oplus$). Untuk $1 \le i \le 7$, tentukan *share* $S_i = \left\langle a_{i,(1,2)}, ..., a_{i,(j_1,j_2)}, ..., a_{i,(n-3+2,...,n)}, a_i \right\rangle$ untuk $1 \le j_1 < j_2 \le 7$ dimana:

$$a_{i,(j_1,j_2)} = \begin{cases} y_{(j_1,j_2)} + h(a_{j_1} \oplus a_{j_2}), \text{ jika } \{p_i, p_{j_1}, p_{j_2}\} \in E(H); \\ \text{kosong, untuk lainnya} \end{cases}$$

Share S_i dengan nilai *subshare* dari masing-masing partisipan p_i dari skema *3-SAH* berdasarkan Gambar 3.1 tercantum pada Tabel 3.2.

Share dari konstruksi skema *3-SAH* berdasarkan Gambar 3.1 dengan nilai *subshare* seperti yang terlihat pada Tabel 3.2 dapat direkonstruksi untuk memperoleh nilai kunci rahasia *K*. Berikut adalah proses rekonstruksi dari skema *3-SAH* dari Contoh 3.5:

a) Untuk $A \subseteq P$ dan $|A| < 3$

Untuk $|A| = 1$ misalnya diambil $A = \{p_3\}$, maka dari Tabel 3.2 , *share* dari p_3 adalah:

$S_3 = \langle 313,-,250,-,-,-,-,167,-,-,-,-,-,-,-,302,302,-,155,-,-,57 \rangle$.

Karena $|A| = 1$, maka *A* tidak mempunyai informasi $y_{(j_1,j_2)}$ untuk semua $1 \le j_1 < j_2 \le 7$. Sehingga dari Tabel 3.2, partisipan p_3 tidak dapat merekonstruksi kunci rahasia *K*.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Untuk $|A| = 2$ misalkan diambil $A = \{p_1, p_2\}$. Maka dari Tabel 3.2 *share* dari p_1 adalah $S_1 = \langle -,-,-,-,-,-,265,167,-,187,-,3,-,-,-,-,-,-,-,-,-,31 \rangle$, sedangkan *share* dari p_2 adalah $S_2 = \langle -,151,250,-,277,-,-,-,-,-,-,3,-,-,-,-,-,-,-,-,-,45 \rangle$. Sehingga dari Tabel 3.1 pada kolom S_1 dan S_2, tidak ada informasi tentang $y_{(1,2)}$ yang diperoleh. Hal ini menunjukkan bahwa partisipan p_1, p_2 tidak dapat merekonstruksi kunci rahasia *K*.

b) Untuk $e \not\subset A \subseteq P \forall e \in \Gamma_0$ dan $|A| \geq 3$

Untuk $|A| = 3$, misalkan diambil $A = \{p_1, p_4, p_6\}$. Maka *share* dari p_1 adalah $S_1 = \langle -,-,-,-,-,-,265,167,-,187,-,3,-,-,-,-,-,-,-,-,-,31 \rangle$, *share* dari p_4 adalah $S_4 = \langle 313,151,-,-,-,-,265,-,-,-,-,-,82,275,-,-,-,-,-,-,-,63 \rangle$, sedangkan *share* dari p_6 adalah $S_6 = \langle 313,-,-,-,-,-,-,-,-,-,-,3,82,-,-,-,-,-,-,-,-,82 \rangle$. Informasi *share* dari *A* yang mungkin diperoleh adalah $y_{(1,4)}, y_{(1,6)}, y_{(4,6)}$. Karena $\{p_1, p_4, p_6\} \notin \Gamma_0$ dari Tabel 3.1 terlihat pada kolom *share* S_1, S_4, dan S_6, tidak ada informasi tentang $y_{(1,4)}, y_{(1,6)}, y_{(4,6)}$ yang dapat diperoleh. Sehingga partisipan p_1, p_4, p_6 tidak dapat merekonstruksi kunci rahasia *K*.

Untuk $|A| > 3$, misalkan diambil $A = \{p_1, p_3, p_6, p_7\}$. Maka *share* dari p_1, p_3, p_6, p_7 adalah:

$S_1 = \langle -,-,-,-,-,-,265,167,-,187,-,3,-,-,-,-,-,-,-,-,-,31 \rangle$

$S_3 = \langle 313,-,250,-,-,-,-,167,-,-,-,-,-,-,-,302,302,-,155,-,-,57 \rangle$

$S_6 = \langle 313,-,-,-,-,-,-,-,-,-,-,3,82,-,-,-,-,-,-,-,-,82 \rangle$

$S_7 = \langle -,96 \rangle$

Informasi *share* dari *A* yang mungkin diperoleh adalah $y_{(1,3)}, y_{(1,6)}, y_{(1,7)}, y_{(3,6)}, y_{(3,7)}, y_{(6,7)}$. Karena *A* tidak memenuhi $e \not\subset A \subseteq P \forall e \in \Gamma_0$, dari Tabel 3.1 terlihat pada kolom S_1, S_3, S_6, S_7, tidak ada informasi mengenai $y_{(1,3)}, y_{(1,6)}, y_{(1,7)}, y_{(3,6)}, y_{(3,7)}, y_{(6,7)}$ yang dapat

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

diperoleh. Sehingga partisipan p_1, p_3, p_6, p_7 tidak dapat merekonstruksi kunci rahasia *K*.

c) Untuk $\exists e \in \Gamma_0, e \subseteq A \subseteq P$ dan $|A| \geq 3$

Misalkan diambil $A = \{p_1, p_2, p_4\}$, hal ini memenuhi $\{p_1, p_2, p_4\} = e \subseteq A$, untuk sembarang $e \in \Gamma_0$. Maka *share* dari p_1 adalah $S_1 = \langle -,-,-,-,-,-,-,265,167,-,187,-,3,-,-,-,-,-,-,-,-,-,-,31 \rangle$, *share* dari p_2 adalah $S_2 = \langle -,151,250,-,277,-,-,-,-,-,-,3,-,-,-,-,-,-,-,-,-,-,45 \rangle$, sedangkan *share* dari p_4 adalah $S_4 = \langle 313,151,-,-,-,-,-,265,-,-,-,-,-,82,275,-,-,-,-,-,-,-,-,63 \rangle$. Informasi *share* dari *A* yang mungkin diperoleh adalah $y_{(1,2)}, y_{(1,4)}, y_{(2,4)}$. Dari Tabel 3.1 pada kolom *share* S_1, S_2, dan S_4, diperoleh nilai dari $a_{1,(2,4)} = 167$, $a_{2,(1,4)} = 250$, dan $a_{4,(1,2)} = 313$. Sedangkan nilai dari a_1, a_2, a_4 adalah berturut-turut 31, 45, dan 63. Berdasarkan Tabel 3.1 maka informasi dari $y_{(1,2)}, y_{(1,4)}, y_{(2,4)}$ dapat diperoleh yaitu $y_{(1,2)} = 263$, $y_{(1,4)} = 218$, dan $y_{(2,4)} = 149$.

Dari nilai $y_{(1,2)}, y_{(1,4)}, y_{(2,4)}$ yang sudah diperoleh selanjutnya dilakukan proses rekonstruksi untuk memperoleh nilai kunci rahasia *K*.

Proses rekonstruksinya sesuai dengan Sub-bab 3.1 adalah sebagai berikut:

Langkah 1 dan **Langkah 2** telah dilakukan sehingga diperoleh nilai dari $y_{(1,2)}, y_{(1,4)}, y_{(2,4)}$.

Langkah 3: Koleksi 3 titik-titik $\left(\sum_{k=1}^{2} i_k n^{3-k-1}, y_{(i_1,i_2)} \right)$ dari langkah 2, yaitu $(9,263)$, $(11,218)$, $(18,149)$. Dari 3 titik tersebut diperoleh $f(9) = 263$, $f(11) = 218$ dan $f(18) = 149$, sehingga bentuk polinomial $f(x) = K_0 + K_1 x + k_2 x^2$ yang diperoleh adalah:

$f(9) = K_0 + 9K_1 + 81k_2$, $f(11) = K_0 + 11K_1 + 121k_2$ dan $f(18) = K_0 + 18K_1 + 324k_2$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Langkah 4: Untuk mencari informasi rahasia K dari persamaan yang diperoleh dari langkah 3 maka digunakan sistem persamaan liniear (SPL). Semua perhitungan dalam langkah rekonstruksi skema *3-SAH* dari Contoh 3.5 ini menggunakan modulo 331. Dengan *SPL* maka diperoleh nilai K_0, K_1, dan k_2 yaitu $K_0 = 179,\ K_1 = 241,\ k_2 = 293$. Sehingga nilai informasi rahasia $K = \{K_0, K_1\}$ dapat diperoleh.

Tabel 3.2: Nilai s*hare* dari skema *3-SAH* untuk untuk 7 partisipan

	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$a_{i,(1,2)}$	-	-	313	313	-	313	-
$a_{i,(1,3)}$	-	151	-	151	-	-	-
$a_{i,(1,4)}$	-	250	250	-	-	-	-
$a_{i,(1,5)}$	-	-	-	-	-	-	-
$a_{i,(1,6)}$	-	277	-	-	-	-	-
$a_{i,(1,7)}$	-	-	-	-	-	-	-
$a_{i,(2,3)}$	265	-	-	265	-	-	-
$a_{i,(2,4)}$	167	-	167	-		-	
$a_{i,(2,5)}$	-	-	-	-	-	-	-
$a_{i,(2,6)}$	187	-	-	-	-	-	-
$a_{i,(2,7)}$	-	-	-	-	-	-	-
$a_{i,(3,4)}$	3	3	-	-	3	3	-
$a_{i,(3,5)}$	-	-	-	82	-	82	-
$a_{i,(3,6)}$	-	-	-	275	275	-	-
$a_{i,(3,7)}$	-	-	-	-	-	-	-
$a_{i,(4,5)}$	-	-	302	-	-	-	-
$a_{i,(4,6)}$	-	-	302	-	-	-	-
$a_{i,(4,7)}$	-	-	-	-	-	-	-
$a_{i,(5,6)}$	-	-	155	-	-	-	-
$a_{i,(5,7)}$	-	-	-	-	-	-	-
$a_{i,(6,7)}$	-	-	-	-	-	-	-
a_i	31	45	57	63	70	82	96

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

3.4 *Information Rate* Skema *3-SAH*

Seperti telah dijelaskan pada Bab 2, *information rate* yang dinotasikan dengan ρ, merupakan ukuran tingkat efisiensi dari skema pembagian rahasia yang diukur dari rata-rata informasinya, yaitu perbandingan antara ukuran kunci rahasia dengan ukuran *share* yang terbesar. Menurut Brickell dan Davenport (1991), *information rate* dari skema pembagian rahasia dinyatakan dengan:

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

dimana K menunjukkan informasi rahasia yang didistribusikan kepada partisipan P, sedangkan *share* dari partisipan ke-i ditunjukkan oleh S_i, untuk $i = 1, 2,\ldots,n$.

Dari proses konstruksi skema *3-SAH* pada Contoh 3.5 diketahui kunci rahasia $K = (K_0, K_1,) = (179,\ 241)$, sedangkan ukuran *share* S_i dari masing-masing partisipan p_i, untuk $i = 1,2,...,n$ dapat diketahui dari Tabel 3.2 yaitu $|S_1| = 5$, $|S_2| = 5$, $|S_3| = 7$, $|S_4| = 6$, $|S_5| = 3$, $|S_6| = 4$, $|S_7| = 1$. Maka menurut Brickell dan Davenport (1991), *information rate* dari skema *3-SAH* adalah:

$$\rho = \frac{\log_2 |K|}{\max_i \log_2 |S_i|} = \frac{\log_2 \left(2^9\right)^2}{\log_2 \left(2^9\right)^7} = \frac{2 \times \log_2 \left(2^9\right)}{7 \times \log_2 \left(2^9\right)} = \frac{2}{7}$$

Menurut Wang dan Juan (2007), *information rate* dari skema pembagian rahasia *3-Hypergraph Access* yang berdasarkan suatu hipergraf H akan memenuhi:

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

dimana d_{max} adalah derajat maksimum dari hipergraf H.

Dari Gambar 3.1 diperoleh derajat maksimum dari hipergraf H adalah $d_{\max} = 6$, sehingga *information rate* dari skema *3-SAH* pada Contoh 3.5 adalah:

$$\rho = \frac{2}{d+1} = \frac{2}{6+1} = \frac{2}{7}$$

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Terlihat bahwa *information rate* yang diperoleh sama dengan *information rate* menurut Brickell dan Davenport . Sehingga perhitungan *information rate* dapat menggunakan rumus Brickell dan Davenport maupun Wang dan Juan.

Pada bab selanjutnya dari Tesis ini akan dibahas tentang skema pembagaian rahasia *3-STH* yang meliputi konstruksi, rekonstruksi, *information rat*e serta contoh skema untuk $n = 7$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

BAB 4
SKEMA PEMBAGIAN RAHASIA 3-STRUKTUR TERLARANG HIPERGRAF

Dalam bab 3 telah dijelaskan mengenai skema pembagian rahasia struktur akses tipe I yang berdasarkan hipergraf *3-uniform*, yaitu skema pembagian rahasia 3-Struktur Akses Hipergraf (skema *3-SAH*). Pada Bab ini akan dibahas tentang skema pembagian rahasia 3-Struktur Terlarang Hipergraf atau disingkat dengan skema *3-STH*. Sama seperti skema *3-SAH*, skema *3-STH* juga berdasarkan hipergraf *3-uniform* tetapi struktur akses yang digunakan adalah struktur akses tipe II. Seperti telah dijelaskan pada Bab 2, struktur akses tipe II atau disebut struktur terlarang Δ, mempunyai struktur $\Gamma = 2^P \setminus \Delta$, dimana P menunjukkan himpunan partisipan yang bersesuaian dengan hiperbusur, sedangkan Δ merupakan himpunan partisipan yang tidak bersesuaian dengan hiperbusur dari hipergraf H.

Pada konstruksi skema *3-SAH*, subhimpunan partisipan yang bersesuaian dengan hiperbusur dari hipergraf H dapat mengakses informasi rahasia tetapi pada konstruksi skema *3-STH* , justru subhimpunan partisipan yang bersesuaian dengan hiperbusur tidak dapat mengakses informasi rahasia. Selain itu subhimpunan partisipan yang mempunyai kardinalitas kurang dari tiga atau $|A| < 3$, juga tidak dapat mengakses informasi rahasia.

Penjelasan mengenai konstruksi skema *3-STH* dalam bab ini diambil dari paper Weng dan Juan (2005).

4.1 Konstruksi Skema *3-STH*

Misalkan suatu hipergraf $H = (P, S)$ dengan $P = \{p_1, p_2, ..., p_n\}$ adalah himpunan partisipan dari skema pembagian rahasia yang bersesuaian dengan simpul-simpul hipergraf H, sedangkan S merupakan himpunan r-partisipan yang bersesuaian dengan hiperbusur dalam H. Dalam konstruksi skema *3-STH*, himpunan dari *3* partisipan yang bersesuaian dengan hiperbusur dalam hipergraf H dinyatakan dengan $S = \{A : A \in E(H)\}$. Sedangkan himpunan dari *3* partisipan yang tidak berada dalam S dinotasikan dengan R

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

yaitu $R = \{A : A \notin E(H) \text{ dan } |A| = 3\}$. Struktur terlarang-nya ditunjukkan oleh $\Delta = \{A : A \subseteq P \text{ dan } |A| \leq 2\} \cup \{A : A \in S\}$. Himpunan partisipan yang terdapat dalam struktur terlarang Δ tidak dapat merekonstruksi kunci rahasia *K*, sedangkan struktur akses dari skema *3-STH* adalah $\Gamma = 2^P \setminus \Delta = \{A : A \subseteq P \text{ dan } |A| \geq 4\} \cup \{A : A \in R\}$. Selanjutnya didefinisikan suatu himpunan T yang menyatakan himpunan partisipan ke-*i* dimana terdapat 3 partisipan lain yang membentuk hiperbusur dan kombinasi 2 diantaranya dengan partisipan ke-*i* juga membentuk hiperbusur, yang dinyatakan sebagai: $T = \{p_i : \exists\, p_j, p_k, p_l \in P \ni \{p_i, p_j, p_k\}, \{p_i, p_j, p_l\}, \{p_i, p_k, p_l\}, \{p_j, p_k, p_l\} \in E(H) \text{ dan } 1 \leq i \neq j \neq k \neq l \leq n\}$.

Seperti pada skema *3-SAH*, konstruksi skema *3-STH* juga menggunakan operasi *exclusive or* (*x-or*) yang dinotasikan dengan $\oplus$ dan suatu fungsi satu arah *hash* (g_{hash}). Kunci rahasia *K* dari skema *3-STH* dinyatakan dengan $K = \{K_0, K_1, K_2\}$ dimana K_0 dan K_1 dan K_2 diambil dari bilangan acak Z_q. Semua perhitungan dalam konstruksi skema *3-STH* dilakukan atas lapangan Z_q, dengan $q \geq \max\{K_0, K_1, K_2\}$ adalah bilangan prima yang besar.

Berikut adalah langkah-langkah dalam konstruksi skema *3-STH*:

Langkah 1:

Misalkan kunci rahasia $K = \{K_0, K_1, K_2\}$ dimana K_0, K_1 dan K_2 diambil secara acak dari Z_q. Suatu *dealer D* mengkonstruksi $f(x) = K_2x^2 + K_1x + K_0$. Misalkan $y_{(i,j)}$ dihitung dari $f(x)$ yaitu $y_{(i,j)} = f(i.n + j)$ untuk $1 \leq i < j \leq n$ dan $y_j = y_{(0,j)} = f(j)$ untuk $j = 1,2,3$.

Langkah 2:

Dealer D mengkonstruksi 3 skema Shamir's *(4,n)-threshold*, yaitu TS_1, TS_2, TS_3 untuk menyembunyikan y_1, y_2, y_3. Untuk setiap $(4,n) - TS_i$, maka y_i merupakan suatu sub-rahasia dan $s_{i,1}, s_{i,2}, ..., s_{i,n}$ merupakan *n* sub*share*-nya.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Langkah 3:

Dealer D memilih sebanyak n bilangan acak atas Z_q yaitu: $r_1, r_2, ..., r_n$.

Selanjutnya *share* $S_i = \left\langle a_{i,(1,2)}, a_{i,(1,3)}, ..., a_{i,(j,l)}, ..., a_{i,(n-1,n)}, a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4} \right\rangle$ dibagikan kepada partisipan p_i, dimana $1 \le j < l \le n$, dengan ketentuan:

$$a_{i,(j,k)} = \begin{cases} y_{j,k} + g_{hash}(r_j \oplus r_k), \text{ jika } i \notin \{j,k\} \text{ dan } \{p_i, p_j, p_k\} \notin E(H); \\ \text{kosong, untuk lainnya} \end{cases}$$

$$a_{i,j} = \begin{cases} s_{j,i}, \text{ jika } p_i \in T \text{ untuk } j = 1,2,3; \\ \text{kosong, untuk lainnya} \end{cases}$$

$$a_{i,4} = r_i$$

Share S_i untuk partisipan p_i, dengan $i = 1,2,...,7$ pada proses konstruksi skema *3-STH* secara umum dapat dilihat pada Tabel 4.1. Tanda "-" dalam tabel menunjukkan bahwa *subshare*-nya kosong.

Konstruksi skema *3-STH* akan memenuhi kondisi sebagai berikut:

(1) jika $A \subseteq P$ dan $|A| < 3$, maka A tidak akan mempunyai informasi kunci rahasia K.

(2) jika $A \in S$, maka A tidak akan mempunyai informasi kunci rahasia K.

(3) jika $A \in R$ maka A dapat merekonstruksi kunci rahasia K.

(4) jika $A \subseteq P$ dan $|A| \ge 4$, maka A dapat merekonstruksi kunci rahasia K.

Penjelasan mengenai keempat kondisi tersebut akan dibahas pada bagian Analisis Keamanan Skema *3-STH.*

4.2 Rekonstruksi Skema *3-STH*

Proses konstruksi skema pembagian rahasia *3-STH* menghasilkan suatu *share* S_i dari partisipan p_i, untuk $i = 1,2,...,n$. Tabel *share* secara umum dari skema *3-STH* untuk *n = 7* pada hipergraf Gambar 3.1 dapat dilihat pada Tabel 4.1. Dari skema *share* tersebut, dapat direkonstruksi oleh beberapa subhimpunan yang termasuk dalam Γ dengan menggabungkan *share*-nya untuk memperoleh struktur kunci rahasia K. Langkah-langkah proses rekonstruksi skema *3-STH* pada dasarnya sama dengan proses rekonstruksi skema *3-SAH* yaitu:

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Langkah 1: Ambil *share* $S_{j_1}, S_{j_2}, S_{j_3}$ dari partisipan $p_{j_1}, p_{j_2}, p_{j_3}$ untuk $1 \le j_1 < j_2 < j_3 \le n$, dimana $A = \{p_{j_1}, p_{j_2}, p_{j_3}\}$ adalah subset minimal dari *P* yang dapat menyusun atau merekonstruksi kunci rahasia K.

Langkah 2: Ambil $\{i_1, i_2\} = \{j_1, j_2, j_3\} \setminus \{t\}$, untuk $1 \le t \le 3$, kemudian hitung $y_{(i_1,i_2)}$ dengan $y_{(i_1,i_2)} = a_{k,(i_1,i_2)} - g_{hash}(a_{i_1} \oplus a_{i_2})$.

Langkah 3: Kumpulkan 3 titik-titik $\left(\sum_{k=1}^{2} i_k n^{3-k-1}, y_{(i_1,i_2)}\right)$ dari langkah 2. Dengan bantuan *3* titik tersebut, polinomial $f(x) = K_0 + K_1 x + K_2 x^2$ dapat direkonstruksi menggunakan interpolasi Lagrange.

Langkah 4: Setelah polinomial $f(x) = K_0 + K_1 x + K_2 x^2$ direkonstruksi, maka informasi rahasia $K = \{K_0, K_1, K_2\}$ dapat diperoleh.

4.3 Analisis Keamanan Skema *3-STH*

Seperti telah disebutkan pada subbab 4.1, konstruksi skema *3-STH* akan memenuhi 4 kondisi. Dua kondisi pertama yaitu jika $A \subseteq P$ dan $|A| < 3$, serta jika $A \in S$, maka A tidak akan mempunyai informasi kunci rahasia *K*. Sedangkan dua kondisi terakhir yaitu jika $A \in R$, serta jika $A \subseteq P$ dan $|A| \ge 4$, maka *A* dapat merekonstruksi kunci rahasia *K*. Analisis keamanan skema *3-STH* berikut ini akan menjelaskan mengenai keempat kondisi tersebut serta *information rate* dari skema *3-STH*.

Teorema 4.1: Untuk semua $A \subseteq P$ dan $|A| < 3$, maka A tidak akan mempunyai informasi kunci rahasia K.

Bukti:

Kasus 1: Jika $|A| = 1$ dan asumsikan $A = \{p_i\}$, dimana $1 \le i \le n$. *Share* dari p_i adalah $S_i = \langle a_{i,(1,2)}, a_{i,(1,3)}, ..., a_{i,(n-1,n)}, a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4} \rangle$. Karena

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

$|A| = 1$, dari elemen-elemen *share* S_i yang ada tidak diperoleh informasi tentang $y_{(j,k)}$ untuk semua $0 \le j < k \le n$. Sehingga partisipan p_i tidak dapat merekonstuksi kunci rahasia *K*.

Kasus 2: Jika $|A| = 2$ dan misalkan $A = \{p_i, p_j\}$, dimana $1 \le i < j \le n$. *Share* dari p_i adalah $S_i = \langle a_{i,(1,2)}, a_{i,(1,3)}, ..., a_{i,(n-1,n)}, a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4} \rangle$. Sedangkan *share* dari p_j ditunjukkan oleh $S_j = \langle a_{j,(1,2)}, a_{j,(1,3)}, ..., a_{j,(n-1,n)}, a_{j,1}, a_{j,2}, a_{j,3}, a_{j,4} \rangle$. Dari kedua *share* ini tidak ada informasi tentang $y_{(i,j)}$ untuk semua $0 \le i < j \le n$ yang diperoleh dari S_i dan S_j. Akibatnya partisipan p_i dan p_j tidak dapat merekonstuksi kunci rahasia *K*. □

Teorema 4.2: Untuk semua $A \in S$, maka *A* tidak akan mempunyai informasi kunci rahasia *K*.

Bukti:

Misalkan $A = \{p_i, p_j, p_k\}$ dengan $1 \le i < j < k \le n$. *Share* dari p_t untuk semua $t \in \{i, j, k\}$ adalah $S_t = \langle a_{t,(1,2)}, a_{t,(1,3)}, ..., a_{t,(n-1,n)}, a_{t,1}, a_{t,2}, a_{t,3}, a_{t,4} \rangle$. Karena $A \in S$ maka $\{p_i, p_j, p_k\} \in E(H)$. Informasi *share* dari A yang mungkin diperoleh yaitu $y_{(i,j)}$, $y_{(i,k)}$, $y_{(j,k)}$. Akan tetapi disisi lain partisipan p_i mempunyai $a_{i,4} = r_i$, sedangkan $a_{i,(i,j)}, a_{i,(i,k)}, a_{i,(j,k)}$ kosong. Partisipan p_j mempunyai $a_{j,4} = r_j$, sedangkan $a_{j,(i,j)}, a_{j,(i,k)}, a_{j,(j,k)}$ kosong. Demikian juga dengan partisipan p_k mempunyai $a_{k,4} = r_k$, sedangkan $a_{k,(i,j)}, a_{k,(i,k)}, a_{k,(j,k)}$ kosong. Akibatnya informasi $y_{(i,j)}$, $y_{(i,k)}$, $y_{(j,k)}$ tidak dapat diperoleh, artinya *A* tidak dapat merekonstruksi kunci rahasia *K*. □

Teorema 4.3: Untuk semua $A \in R$ maka *A* dapat merekonstruksi kunci rahasia *K*.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Bukti:

Misalkan $A = \{p_i, p_j, p_k\}$ dengan $1 \le i < j < k \le n$. *Share* dari p_t untuk semua $t \in \{i, j, k\}$ adalah $S_t = \langle a_{t,(1,2)}, a_{t,(1,3)}, ..., a_{t,(n-1,n)}, a_{t,1}, a_{t,2}, a_{t,3}, a_{t,4} \rangle$. Karena $A \in R$, $\{p_i, p_j, p_k\} \notin E(H)$, maka partisipan p_i mempunyai $a_{i,4} = r_i$ dan $a_{i,(j,k)} = y_{(j,k)} + g(r_j \oplus r_k)$. Partisipan p_j mempunyai $a_{j,4} = r_j$ dan $a_{j,(i,k)} = y_{(i,k)} + g(r_i \oplus r_k)$. Partisipan p_k mempunyai $a_{k,4} = r_k$ dan $a_{k,(i,j)} = y_{(i,j)} + g(r_i \oplus r_j)$. Dengan ketiga *share* ini, informasi $y_{(i,j)}$, $y_{(i,k)}$, $y_{(j,k)}$ dapat diperoleh, sehingga *f(x)* dapat ditentukan dan kunci rahasia *K* dapat direkonstruksi. □

Teorema 4.4: Untuk semua $A \subseteq P$ dan $|A| \ge 4$, maka A dapat merekonstruksi kunci rahasia *K*.

Bukti:

Misalkan $A = \{p_i, p_j, p_k, p_l\}$ dengan $1 \le i < j < k < l \le n$. Jika terdapat 3 partisipan dari *A* yang dimiliki oleh *R*, maka menurut Teorema 4.3 kunci rahasia *K* dapat direkonstruksi. Hal ini juga berlaku untuk semua $\{p_i, p_j, p_k\}, \{p_i, p_j, p_l\}, \{p_i, p_k, p_l\}, \{p_j, p_k, p_l\}$ yang merupakan hiperbusur dari *H*. Jika demikian maka partisipan $p_i, p_j, p_k, p_l \in T$. Hal ini akan mengakibatkan partisipan p_t memiliki $a_{t,1} = s_{1,t}$, $a_{t,2} = s_{2,t}$ dan $a_{t,3} = s_{3,t}$ untuk semua $t \in \{i, j, k, l\}$, sehingga p_i, p_j, p_k, p_l dapat merekonstruksi $y_1, y_2,$ dan y_3. Karena $y_1 = SK_1$, $y_2 = SK_2$, dan $y_3 = SK_3$, selanjutnya sub rahasia SK_1, SK_2, dan SK_3 akan digunakan untuk merekonstruksi kunci rahasia *K* dari persamaan $f(x) = K_2 x^2 + K_1 x + K_0$. Sehingga kunci rahasia *K* dapat diperoleh. □

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Teorema 4.5: Misalkan *n* adalah banyaknya simpul-simpul dari hipergraf *H* dan *d* merupakan derajat minimum dari hipergraf *H*, maka *information rate* ρ dari skema *3-STH* adalah:

1) $3/\left(C(n-1,2)-d+4\right) \le \rho \le 3/\left(C(n-1,2)-d+1\right)$, jika $d \ge 3$

2) $\rho \ge 3/\left(C(n-1,2)+1\right)$

Bukti:

Suatu *share* S_i dari partisipan p_i adalah suatu vektor dengan elemen $\left(C(n,2)+4\right)$. Untuk elemen $C(n,2)$ pertama, jika $\left\{p_{l_1}, p_{l_2}, p_{l_3}\right\} \in E(H)$ dimana $1 \le l_1 < l_2 < l_3 \le n$, maka $a_{l_i,(x_1,x_2)}$ kosong untuk setiap $l_i \in \{x_1, x_2\} \subseteq \{1,2,...,n\}$ atau $\{x_1, x_2\} = \{l_1, l_2, l_3\} - \{l_i\}$. Sedangkan $a_{l_i,(x_1,x_2)}$ yang lainnya atas Z_q.

Untuk elemen terakhir yaitu 4, nilai $a_{l_i,4}$ selalu sama dengan r_i untuk $i = 1,2,...,n$; sedangkan masing-masing nilai $a_{l_i,j}$ untuk $1 \le j \le 3$ adalah atas Z_q atau bisa saja bernilai kosong, tergantung dari p_i apakah dalam himpunan T atau tidak. Karena itu, ukuran *share* Sl_i paling besar adalah $\log\left(q^{C(n-1,2)-\deg(p_{l_i})+4}\right)$ pada saat $a_{l_i,j}$ tidak kosong untuk $1 \le j \le 3$; dan paling sedikit $\log\left(q^{C(n-1,2)-\deg(p_{l_i})+1}\right)$ ketika $a_{l_i,j}$ kosong untuk $1 \le j \le 3$, dimana $\deg(p_{l_i})$ adalah derajat dari simpul p_{l_i} dalam hipergraf *H*. Sehingga ukuran maksimal dari *share*-nya adalah paling besar $\log\left(q^{C(n-1,2)-d+4}\right)$ dan paling kecil $\log\left(q^{C(n-1,2)-d+1}\right)$, dimana d merupakan derajat terkecil dari H.

Karena ukuran dari kunci rahasia adalah $\log\left(q^3\right)$, maka *information rate* dari skema *3-STH* akan memenuhi:

$$(3\log q)/\left(\left(C(n-1,2)-d+4\right)\log q\right) \le \rho \le (3\log q)/\left(\left(C(n-1,2)-d+1\right)\log q\right).$$

Untuk membuktikan 2), nilai $a_{i,j}$ adalah tidak kosong untuk $1 \le j \le 3$, sedemikian sehingga $p_i, p_{l_1}, p_{l_2}, p_{l_3}$ memenuhi $\left\{p_{x_1}, p_{x_2}, p_{x_3}\right\} \in H$ dimana

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

$\{x_1, x_2, x_3\} \subseteq \{i, l_1, l_2, l_3\}$. Sehingga $a_{i,(x_1,x_2,x_3)}$ kosong. Hal ini berarti $\deg(p_i) \geq 3$, sehingga *information rate* $\rho \geq 3/(C(n-1,2)+1)$ terpenuhi. □

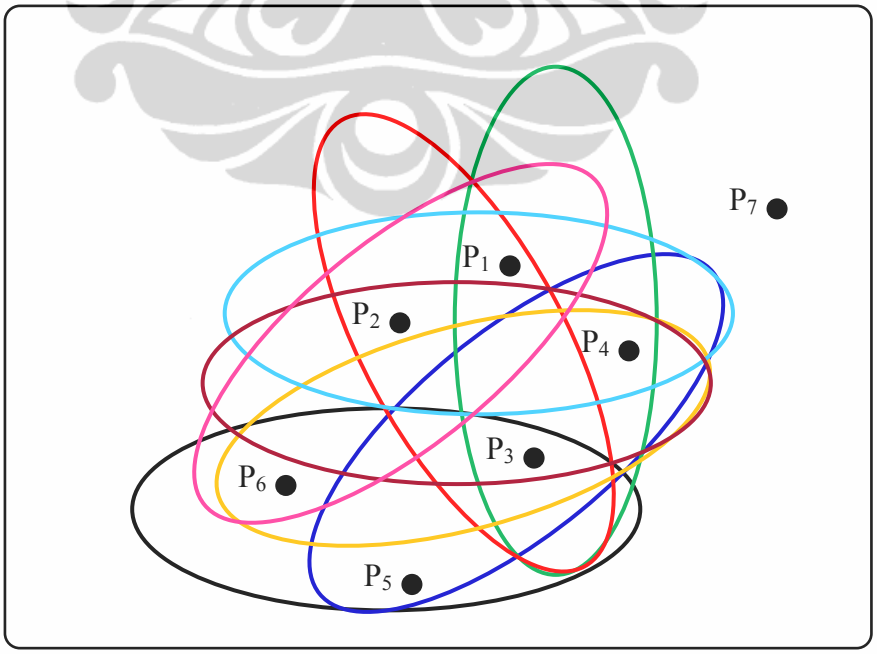
Akibat 4.6: Batas terendah *information rate* skema *3-STH* adalah $\max\{3/(C(n-1,2)-d+4),\ 3/(C(n-1,2)+1)\}$, dimana d merupakan derajat minimum dari hipergraf H sedangkan n adalah banyaknya simpul-simpul dari H.

S*hare* dari skema *3-HST* secara umum untuk 7 partisipan berdasarkan hipergraf Gambar 4.1 dapat dilihat pada Tabel 4.1 .

Gambaran yang lebih jelas dalam proses konstruksi dan rekonstruksi pembentukan skema pembagian rahasia *3-STH* diberikan pada Contoh 4.7 berikut ini.

Contoh 4.7:

Contoh proses konstruksi dan rekonstruksi pembentukan skema *3-STH* berikut ini menggunakan hipergraf pada Gambar 3.1. Untuk mempermudah hipergraf ini diberikan kembali pada Gambar 4.1.



Gambar 4.1
Contoh *3-Uniform* Hipergraf *H*

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Tabel 4.1: *Share* Secara Umum dari Skema *3-STH* untuk Hipergraf pada Gambar 4.1

	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$a_{i,(1,2)}$	-	-	-	-	$y_{(1,2)} + g_{hash}(r_1 \oplus r_2)$	-	$y_{(1,2)} + g_{hash}(r_1 \oplus r_2)$
$a_{i,(1,3)}$	-	-	-	-	$y_{(1,3)} + g_{hash}(r_1 \oplus r_3)$	$y_{(1,3)} + g_{hash}(r_1 \oplus r_3)$	$y_{(1,3)} + g_{hash}(r_1 \oplus r_3)$
$a_{i,(1,4)}$	-	-	-	-	$y_{(1,4)} + g_{hash}(r_1 \oplus r_4)$	$y_{(1,4)} + g_{hash}(r_1 \oplus r_4)$	$y_{(1,4)} + g_{hash}(r_1 \oplus r_4)$
$a_{i,(1,5)}$	-	$y_{(1,5)} + g_{hash}(r_1 \oplus r_5)$	$y_{(1,5)} + g_{hash}(r_1 \oplus r_5)$	$y_{(1,5)} + g_{hash}(r_1 \oplus r_5)$	-	$y_{(1,5)} + g_{hash}(r_1 \oplus r_5)$	$y_{(1,5)} + g_{hash}(r_1 \oplus r_5)$
$a_{i,(1,6)}$	-	-	$y_{(1,6)} + g_{hash}(r_1 \oplus r_6)$	$y_{(1,6)} + g_{hash}(r_1 \oplus r_6)$	$y_{(1,6)} + g_{hash}(r_1 \oplus r_6)$	-	$y_{(1,6)} + g_{hash}(r_1 \oplus r_6)$
$a_{i,(1,7)}$	-	$y_{(1,7)} + g_{hash}(r_1 \oplus r_7)$	$y_{(1,7)} + g_{hash}(r_1 \oplus r_7)$	$y_{(1,7)} + g_{hash}(r_1 \oplus r_7)$	$y_{(1,7)} + g_{hash}(r_1 \oplus r_7)$	$y_{(1,7)} + g_{hash}(r_1 \oplus r_7)$	-
$a_{i,(2,3)}$	-	-	-	-	$y_{(2,3)} + g_{hash}(r_2 \oplus r_3)$	$y_{(2,3)} + g_{hash}(r_2 \oplus r_3)$	$y_{(2,3)} + g_{hash}(r_2 \oplus r_3)$
$a_{i,(2,4)}$	-	-	-	-	$y_{(2,4)} + g_{hash}(r_2 \oplus r_4)$	-	$y_{(2,4)} + g_{hash}(r_2 \oplus r_4)$
$a_{i,(2,5)}$	$y_{(2,5)} + g_{hash}(r_2 \oplus r_5)$	-	$y_{(2,5)} + g_{hash}(r_2 \oplus r_5)$	$y_{(2,5)} + g_{hash}(r_2 \oplus r_5)$	-	$y_{(2,5)} + g_{hash}(r_2 \oplus r_5)$	$y_{(2,5)} + g_{hash}(r_2 \oplus r_5)$
$a_{i,(2,6)}$	-	-	$y_{(2,6)} + g_{hash}(r_2 \oplus r_6)$	$y_{(2,6)} + g_{hash}(r_2 \oplus r_6)$	$y_{(2,6)} + g_{hash}(r_2 \oplus r_6)$	-	$y_{(2,6)} + g_{hash}(r_2 \oplus r_6)$
$a_{i,(2,7)}$	$y_{(2,7)} + g_{hash}(r_2 \oplus r_7)$	-	$y_{(2,7)} + g_{hash}(r_2 \oplus r_7)$	$y_{(2,7)} + g_{hash}(r_2 \oplus r_7)$	$y_{(2,7)} + g_{hash}(r_2 \oplus r_7)$	$y_{(2,7)} + g_{hash}(r_2 \oplus r_7)$	-
$a_{i,(3,4)}$	-	-	-	-	-	-	$y_{(3,4)} + g_{hash}(r_3 \oplus r_4)$
$a_{i,(3,5)}$	$y_{(3,5)} + g_{hash}(r_3 \oplus r_5)$	$y_{(3,5)} + g_{hash}(r_3 \oplus r_5)$	-	-	-	-	$y_{(3,5)} + g_{hash}(r_3 \oplus r_5)$
$a_{i,(3,6)}$	$y_{(3,6)} + g_{hash}(r_3 \oplus r_6)$	$y_{(3,6)} + g_{hash}(r_3 \oplus r_6)$	-	-	-	-	$y_{(3,6)} + g_{hash}(r_3 \oplus r_6)$
$a_{i,(3,7)}$	$y_{(3,7)} + g_{hash}(r_3 \oplus r_7)$	$y_{(3,7)} + g_{hash}(r_3 \oplus r_7)$	-	$y_{(3,7)} + g_{hash}(r_3 \oplus r_7)$	$y_{(3,7)} + g_{hash}(r_3 \oplus r_7)$	$y_{(3,7)} + g_{hash}(r_3 \oplus r_7)$	-
$a_{i,(4,5)}$	$y_{(4,5)} + g_{hash}(r_4 \oplus r_5)$	$y_{(4,5)} + g_{hash}(r_4 \oplus r_5)$	-	-	-	$y_{(4,5)} + g_{hash}(r_4 \oplus r_5)$	$y_{(4,5)} + g_{hash}(r_4 \oplus r_5)$
$a_{i,(4,6)}$	$y_{(4,6)} + g_{hash}(r_4 \oplus r_6)$	$y_{(4,6)} + g_{hash}(r_4 \oplus r_6)$	-	-	$y_{(4,6)} + g_{hash}(r_4 \oplus r_6)$	-	$y_{(4,6)} + g_{hash}(r_4 \oplus r_6)$
$a_{i,(4,7)}$	$y_{(4,7)} + g_{hash}(r_4 \oplus r_7)$	$y_{(4,7)} + g_{hash}(r_4 \oplus r_7)$	$y_{(4,7)} + g_{hash}(r_4 \oplus r_7)$	-	$y_{(4,7)} + g_{hash}(r_4 \oplus r_7)$	$y_{(4,7)} + g_{hash}(r_4 \oplus r_7)$	-
$a_{i,(5,6)}$	$y_{(5,6)} + g_{hash}(r_5 \oplus r_6)$	$y_{(5,6)} + g_{hash}(r_5 \oplus r_6)$	-	$y_{(5,6)} + g_{hash}(r_5 \oplus r_6)$	-	-	$y_{(5,6)} + g_{hash}(r_5 \oplus r_6)$
$a_{i,(5,7)}$	$y_{(5,7)} + g_{hash}(r_5 \oplus r_7)$	$y_{(5,7)} + g_{hash}(r_5 \oplus r_7)$	$y_{(5,7)} + g_{hash}(r_5 \oplus r_7)$	$y_{(5,7)} + g_{hash}(r_5 \oplus r_7)$	-	$y_{(5,7)} + g_{hash}(r_5 \oplus r_7)$	-
$a_{i,(6,7)}$	$y_{(6,7)} + g_{hash}(r_6 \oplus r_7)$	$y_{(6,7)} + g_{hash}(r_6 \oplus r_7)$	$y_{(6,7)} + g_{hash}(r_6 \oplus r_7)$	$y_{(6,7)} + g_{hash}(r_6 \oplus r_7)$	$y_{(6,7)} + g_{hash}(r_6 \oplus r_7)$	-	-
$a_{i,1}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,4}$	-	-	-
$a_{i,2}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$	$s_{2,4}$	-	-	-
$a_{i,3}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$	$s_{3,4}$	-	-	-
$a_{i,4}$	r_1	r_2	r_3	r_4	r_5	r_6	r_7

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Himpunan partisipan yang bersesuaian dengan simpul-simpul pada hipergraf H adalah $P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$. Himpunan dari *3* partisipan yang bersesuaian dengan hiperbusur yaitu $E(H) = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_2, p_6\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}, \{p_3, p_4, p_5\}, \{p_3, p_4, p_6\}, \{p_3, p_5, p_6\}\}$. Sedangkan himpunan partisipan yang tidak berada dalam S dituliskan sebagai $R = \{\{p_1, p_2, p_5\}, \{p_1, p_2, p_7\}, \{p_1, p_3, p_5\}, \{p_1, p_3, p_6\}, \{p_1, p_3, p_7\}, \{p_1, p_4, p_5\}, \{p_1, p_4, p_6\}\{p_1, p_4, p_7\}, \{p_1, p_5, p_6\}, \{p_1, p_5, p_7\}, \{p_1, p_6, p_7\}, \{p_2, p_3, p_5\}, \{p_2, p_3, p_6\}, \{p_2, p_3, p_7\}, \{p_2, p_4, p_5\}, \{p_2, p_4, p_6\}, \{p_2, p_4, p_7\}, \{p_2, p_5, p_6\}, \{p_2, p_5, p_7\}, \{p_2, p_6, p_7\}, \{p_3, p_4, p_7\}, \{p_3, p_5, p_7\}, \{p_3, p_6, p_7\}, \{p_4, p_5, p_6\}, \{p_4, p_5, p_7\}, \{p_4, p_6, p_7\}, \{p_5, p_6, p_7\}\}$.

Struktur terlarang dari skema *3-STH* ditunjukkan oleh

$\Delta = \{\phi, \{p_1\}, \{p_2\}, \{p_3\}, \{p_4\}, \{p_5\}, \{p_6\}, \{p_7\}, \{p_1, p_2\}, \{p_1, p_3\}, \{p_1, p_4\}, \{p_1, p_5\}, \{p_1, p_6\}, \{p_1, p_7\}, \{p_2, p_3\}, \{p_2, p_4\}, \{p_2, p_5\}, \{p_2, p_6\}, \{p_2, p_7\}, \{p_3, p_4\}, \{p_3, p_5\}, \{p_3, p_6\}, \{p_3, p_7\}, \{p_4, p_5\}, \{p_4, p_6\}, \{p_4, p_7\}, \{p_5, p_6\}, \{p_5, p_7\}, \{p_6, p_7\}\} \cup S$.

Struktur akses skema *3-STH* adalah $\Gamma = 2^P \setminus \Delta = \{A : A \subseteq P \text{ dan } |A| \geq 4\} \cup \{A : A \in R\}$, sedangkan himpunan T dinyatakan dengan:

$T = \{p_i : \exists p_j, p_k, p_l \in P \ni \{p_i, p_j, p_k\}, \{p_i, p_j, p_l\}, \{p_i, p_k, p_l\}, \{p_j, p_k, p_l\} \in E(H) \quad \text{dan } 1 \leq i \neq j \neq k \neq l \leq n\}$.

Konstruksi skema *3-STH* dilakukan dengan langkah-langkah berikut:

Langkah 1:

Misalkan kunci rahasia $K = \{K_0, K_1, K_2\}$, dimana $K_0 = 179$, $K_1 = 241$, dan $K_2 = 293$, diambil secara acak dari Z_{331}. *Dealer D* mengkonstruksi $f(x) = K_2x^2 + K_1x + K_0$ yaitu $f(x) = 293x^2 + 241x + 179$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Misalkan $y_{(i,j)}$ dihitung dari $f(x)$ yaitu $y_{(i,j)} = f(i.n + j)$ untuk $1 \le i < j \le 7$, sedangkan $y_{(j)} = y_{(0,j)} = f(j) (\text{mod}\, 331)$ untuk *j=1,2,3*.

Langkah 2:

Dealer D mengkonstruksi 3 skema Shamir's *(4, n)-threshold*, yaitu TS_1, TS_2, TS_3 untuk menyembunyikan nilai y_1, y_2, y_3. Untuk setiap $(4,n) - TS_i$ dengan *i=1,2,3*, maka y_i merupakan suatu *sub*-rahasia dan $s_{i,1}, s_{i,2}, ..., s_{i,n}$ merupakan *n subshare*-nya. Jadi:

$y_{(1)} = f(1) (\text{mod}\, 331) = 51$ adalah *sub*rahasia SK_1

$y_{(2)} = f(2) (\text{mod}\, 331) = 178$ adalah *sub*rahasia SK_2

$y_{(3)} = f(3) (\text{mod}\, 331) = 229$ adalah *sub*rahasia SK_3

Selanjutnya dikonstruksi tiga skema *(4,7)-threshold* untuk melindungi sub rahasia SK_1, SK_2, SK_3, yaitu:

$TS_1 = 32x^3 + 20x^2 + 15x + 51$

$TS_2 = 77x^3 + 60x^2 + 45x + 178$

$TS_3 = 50x^3 + 40x^2 + 32x + 229$

Sub*share* dari TS_1 adalah $s_{1,1}, s_{1,2}, ..., s_{1,7}$

Sub*share* dari TS_2 adalah $s_{2,1}, s_{2,2}, ..., s_{2,7}$

Sub*share* dari TS_3 adalah $s_{3,1}, s_{3,2}, ..., s_{3,7}$

Langkah 3:

Dealer D memilih sebanyak *7* bilangan acak atas Z_{331} yaitu:

$r_1 = 31,\ r_2 = 45,\ r_3 = 57,\ r_4 = 63,\ r_5 = 70,\ r_6 = 82,\ r_7 = 96$.

Selanjutnya *share* dari partisipan p_i untuk $i = 1, 2, ..., 7$, diperoleh dari

$S_i = \langle a_{i,(1,2)}, a_{i,(1,3)}, ..., a_{i,(j,l)}, ..., a_{i,(n-1,n)}, a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4} \rangle$, untuk $1 \le j < l \le 7$,

dengan ketentuan:

$$a_{i,(j,k)} = \begin{cases} y_{j,k} + g_{hash}(r_j \oplus r_k), \text{ jika } i \notin \{j,k\} \text{ dan } \{p_i, p_j, p_k\} \notin E(H); \\ \text{kosong, untuk lainnya} \end{cases}$$

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

$$a_{i,j} = \begin{cases} s_{j,i}, \text{ jika } p_i \in T \text{ untuk } j = 1,2,3; \\ \text{kosong, untuk lainnya} \end{cases}$$

$$a_{i,4} = r_i$$

Dalam menentukan *share* dari partisipan pada contoh ini digunakan fungsi satu arah *hash* $\left(g_{hash}\right)$ sederhana yaitu operasi operasi *exclusive-or* (*x-or*). Dari persamaan $f(x) = 293x^2 + 241x + 179$ dan $y_{(i,j)} = f\left(i.n + j\right)$ untuk $1 \le i < j \le 7$, maka diperoleh:

$$y_{(1,2)} = f\left(1.7 + 2\right) = f(9) = 263$$

$$y_{(1,3)} = f\left(1.7 + 3\right) = f(10) = 113$$

$$y_{(1,4)} = f\left(1.7 + 4\right) = f(11) = 218$$

$$\vdots$$

$$y_{(6,7)} = f\left(6.7 + 7\right) = f(49) = 190$$

Sedangkan dari konstruksi tiga skema *(4,7)-threshold* yaitu:

$TS_1 = 32x^3 + 20x^2 + 15x + 51$ dengan *subshare*: $s_{1,1}, s_{1,2}, ..., s_{1,7}$.

$TS_2 = 77x^3 + 60x^2 + 45x + 178$ dengan *subshare*: $s_{2,1}, s_{2,2}, ..., s_{2,7}$

$TS_3 = 50x^3 + 40x^2 + 32x + 229$ dengan *subshare* : $s_{3,1}, s_{3,2}, ..., s_{3,7}$

diperoleh nilai subshare dari TS_i dengan i untuk $1 \le i \le 7$ sebagai berikut:

$TS_1(1) = 118$	$TS_2(1) = 29$	$TS_3(1) = 20$
$TS_1(2) = 86$	$TS_2(2) = 131$	$TS_3(2) = 191$
$\vdots$	$\vdots$	$\vdots$
$TS_1(7) = 196$	$TS_2(7) = 54$	$TS_3(7) = 34$

Dengan memilih *7* bilangan acak atas Z_{331} yaitu: $r_1 = 31, r_2 = 45, r_3 = 57, r_4 = 63, r_5 = 70, r_6 = 82, r_7 = 96$, maka diperoleh nilai *share* yang selengkapnya ditampilkan pada Tabel 4.2.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Tabel 4.2: Nilai S*hare* dari Skema *3-STH* untuk 7 Partisipan

	S_1	S_2	S_3	S_4	S_5	S_6	S_7
$a_{i,(1,2)}$	-	-	-	-	313	-	313
$a_{i,(1,3)}$	-	-	-	-	151	151	151
$a_{i,(1,4)}$	-	-	-	-	250	250	250
$a_{i,(1,5)}$	-	5	5	5	-	5	5
$a_{i,(1,6)}$	-	-	277	277	277	-	277
$a_{i,(1,7)}$	-	204	204	204	204	204	-
$a_{i,(2,3)}$	-	-	-	-	265	265	265
$a_{i,(2,4)}$	-	-	-	-	167	-	167
$a_{i,(2,5)}$	84	-	84	84	-	84	84
$a_{i,(2,6)}$	-	-	187	187	187	-	187
$a_{i,(2,7)}$	144	-	144	144	144	144	-
$a_{i,(3,4)}$	-	-	-	-	-	-	3
$a_{i,(3,5)}$	82	82	-	-	-	-	82
$a_{i,(3,6)}$	275	275	-	-	-	-	275
$a_{i,(3,7)}$	63	63	-	63	63	63	-
$a_{i,(4,5)}$	302	302	-	-	-	302	302
$a_{i,(4,6)}$	302	302	-	-	302	-	302
$a_{i,(4,7)}$	224	224	224	-	224	224	-
$a_{i,(5,6)}$	155	155	-	155	-	-	155
$a_{i,(5,7)}$	239	239	239	239	-	239	-
$a_{i,(6,7)}$	240	240	240	240	240	-	-
$a_{i,1}$	118	86	147	162	-	-	-
$a_{i,2}$	29	131	284	288	-	-	-
$a_{i,3}$	20	191	49	225	-	-	-
$a_{i,4}$	31	45	57	63	70	82	96

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Share dari proses konstruksi skema *3-STH* seperti yang terlihat pada Tabel 4.2 dapat direkonstruksi untuk memperoleh nilai kunci rahasia *K*. Proses konstruksi skema *3-STH* pada Contoh 4.7 akan memenuhi:

(1) jika $A \subseteq P$ dan $|A| < 3$, maka *A* tidak akan mempunyai informasi kunci rahasia *K*.

(2) jika $A \in S$, maka *A* tidak akan mempunyai informasi kunci rahasia *K*.

(3) jika $A \in R$ maka *A* dapat merekonstruksi kunci rahasia *K*.

(4) jika $A \subseteq P$ dan $|A| \geq 4$, maka *A* dapat merekonstruksi kunci rahasia *K*.

Berikut adalah proses rekonstruksi dari skema *3-HSA* dari Contoh 4.7:

(1) Untuk semua $A \subseteq P$ dan $|A| < 3$, maka *A* tidak akan mempunyai informasi kunci rahasia *K*.

Kasus 1:

Untuk $|A| = 1$ dan asumsi $A = \{p_i\}$ dimana $1 \leq i \leq 7$; misalnya diambil p_3, maka $A = \{p_3\} \in \Delta$, dimana:

$$\Delta = \{\phi, \{p_1\}, \{p_2\}, \{p_3\}, \{p_4\}, \{p_5\}, \{p_6\}, \{p_7\}, \{p_1, p_2\}, \{p_1, p_3\}, \{p_1, p_4\}, \{p_1, p_5\}, \{p_1, p_6\}\{p_1, p_7\}, \{p_2, p_3\}, \{p_2, p_4\}, \{p_2, p_5\}, \{p_2, p_6\}, \{p_2, p_7\}, \{p_3, p_4\}, \{p_3, p_5\}, \{p_3, p_6\}, \{p_3, p_7\}, \{p_4, p_5\}, \{p_4, p_6\}, \{p_4, p_7\}, \{p_5, p_6\}, \{p_5, p_7\}, \{p_6, p_7\}\} \cup S$$

Dari Tabel 4.2, diperoleh *share* dari p_3 adalah

$S_3 = \langle$-,-,-,5,277,204,-,-,84,187,144,-,-,-,-,-,-,224,-,239,240,147,284,49,57$\rangle$.

Karena $|A| = 1$, maka *A* tidak mempunyai informasi tentang $y_{(j,k)}$ untuk semua $1 \leq j < k \leq 7$, sehingga p_3 tidak dapat merekonstruksi kunci rahasia *K*.

Kasus 2:

Untuk $|A| = 2$ dan asumsi $A = \{p_i, p_j\}$, dimana $1 \leq i < j \leq 7$. Misalnya diambil $A = \{p_3, p_6\}$, maka $A \in \Delta$.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Dari Tabel 4.2, diperoleh *share* dari p_3 adalah

$S_3 = \langle -,-,-,5,277,204,-,-,84,187,144,-,-,-,-,-,-,224,-,239,240,147,284,49,57 \rangle$.

Sedangkan *share* dari p_6 adalah

$S_6 = \langle -,151,250,5,-,204,265,-,84,-,144,-,-,-,63,302,-,224,-,239,-,-,-,-,82 \rangle$.

Dari tabel 4.1 pada kolom S_3 dan S_6, tidak terdapat informasi tentang $y_{(3,6)}$, sehingga partisipan p_3 dan p_6 tidak dapat merekonstuksi kunci rahasia *K*.

(2) Untuk semua $A \in S$, maka *A* tidak akan mempunyai informasi kunci rahasia *K*.

Misalkan $A = \{ p_i, p_j, p_k \}$ dengan $1 \le i < j < k \le n$, diambil

$A = \{ p_1, p_2, p_3 \} \in S$. Dari Tabel 4.2, diperoleh *share* dari p_1, p_2, p_3 adalah:

$S_1 = \langle -,-,-,-,-,-,-,-,84,-,144,-,82,275,63,302,302,224,155,239,240,118,29,20,31 \rangle$

$S_2 = \langle -,-,-,5,-,204,-,-,-,-,-,-,82,275,63,302,302,224,155,239,240,86,131,191,45 \rangle$

$S_3 = \langle -,-,-,5,277,204,-,-,84,187,144,-,-,-,-,-,-,224,-,239,240,147,284,49,57 \rangle$

Karena $A \in S$ maka $\{ p_1, p_2, p_3 \} \in E(H)$. Sehingga informasi *share* dari *A* yang mungkin diperoleh, yaitu $y_{(1,2)}$, $y_{(1,3)}$, $y_{(3,4)}$. Dari Tabel 4.1 dan 4.2 pada kolom S_1, S_2, dan S_3, diperoleh partisipan p_1 mempunyai $a_{1,4} = r_1 = 31$, sedangkan $a_{1,(1,2)}, a_{1,(1,3)}, a_{1,(2,3)}$ kosong. Partisipan p_2 mempunyai $a_{2,4} = r_2 = 45$, sedangkan $a_{2,(1,2)}, a_{2,(1,3)}, a_{2,(2,3)}$ kosong. Partisipan p_3 mempunyai $a_{3,4} = r_3 = 57$, sedangkan $a_{3,(1,2)}, a_{3,(1,3)}, a_{3,(2,3)}$ kosong. Sebagai akibatnya, informasi $y_{(1,2)}$, $y_{(1,3)}$, $y_{(3,4)}$ tidak dapat diperoleh, artinya *A* tidak dapat merekonstruksi kunci rahasia *K*.

(3) Untuk semua $A \in R$ maka *A* dapat merekonstruksi kunci rahasia *K*.

Misalkan $A = \{ p_i, p_j, p_k \}$ dengan $1 \le i < j < k \le n$, diambil

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

$A = \{p_5, p_6, p_7\} \in R$. Dari Tabel 4.2, diketahui share dari p_5, p_6, p_7 adalah:

$S_5 = \langle 313,151,250,-,277,204,265,167,-,187,144,-,-,-,63,-,302,224,-,-,240,-,-,-,70 \rangle$

$S_6 = \langle -,151,250,5,-,204,265,-,84,-,144,-,-,-,63,302,-,224,-,239,-,-,-,-,82 \rangle$

$S_7 = \langle 313,151,250,5,277,-,265,167,84,187,-,3,82,275,-,302,302,-,155,-,-,-,-,-,96 \rangle$

Karena $A \in R$, $\{p_5, p_6, p_7\} \notin E(H)$, dilihat dari Tabel 4.1 dan 4.2, Maka partisipan p_5 mempunyai $a_{5,4} = r_5 = 70$ dan $a_{5,(6,7)} = y_{(6,7)} + g(r_6 \oplus r_7) = 240$. Partisipan p_6 mempunyai $a_{6,4} = r_6 = 82$ dan $a_{6,(5,7)} = y_{(5,7)} + g(r_5 \oplus r_7) = 239$. Sedangkan partisipan p_7 mempunyai $a_{7,4} = r_7 = 96$ dan $a_{7,(5,6)} = y_{(5,6)} + g(r_5 \oplus r_6) = 155$.

Akibatnya informasi $y_{(5,6)}$, $y_{(5,7)}$, $y_{(6,7)}$ dapat diperoleh dengan:

$$a_{5,(6,7)} = y_{(6,7)} + g(r_6 \oplus r_7) = 240$$

$$a_{6,(5,7)} = y_{(5,7)} + g(r_5 \oplus r_7) = 239$$

$$a_{7,(5,6)} = y_{(5,6)} + g(r_5 \oplus r_6) = 155$$

dari persamaan $y_{(i,j)} = f(i.n + j)$ untuk $1 \le i < j \le 7$, dan digunakan fungsi *hash* sederhana *x-or* $(r_j \oplus r_k)$, maka diperoleh:

$$y_{(6,7)} = f(6.7 + 7) = f(49) = 190$$

$$y_{(5,7)} = f(5.7 + 7) = f(42) = 201$$

$$y_{(5,6)} = f(5.7 + 6) = f(41) = 135$$

Selanjutnya dari persamaan $f(x) = K_2 x^2 + K_1 x + K_0$ akan direkonstruksi K_1, K_2 *dan* K_3:

$$f(49) = 84K_2 + 49K_1 + K_0 = 190$$

$$f(42) = 109K_2 + 42K_1 + K_0 = 201$$

$$f(41) = 26K_2 + 41K_1 + K_0 = 135$$

Dengan sistem persamaan linier (*SPL*) maka diperoleh kunci rahasia *K*, yaitu $K_2 = 293,\ K_1 = 241,\ K_0 = 179$

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

(4) Untuk semua $A \subseteq P$ dan $|A| \geq 4$, maka *A* dapat merekonstruksi kunci rahasia *K*.

Misalkan $A = \{p_i, p_j, p_k, p_l\}$ dengan $1 \leq i < j < k < l \leq n$, diambil $A = \{p_1, p_2, p_3, p_4\}$. Jika terdapat 3 partisipan dari *A* yang dimiliki oleh *R*, maka menurut teorema 3 kunci rahasia *K* dapat direkonstruksi. Hal ini juga berlaku untuk $\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}$ yang merupakan hiperbusur dari *H*, sehingga partisipan $p_1, p_2, p_3, p_4 \in T$. Dari Tabel 4.1 dan 4.2 diperoleh partisipan p_1 memiliki $a_{1,1} = s_{1,1} = 118$, $a_{1,2} = s_{2,1} = 29$ dan $a_{1,3} = s_{3,1} = 20$; partisipan p_2 memiliki $a_{2,1} = s_{1,2} = 86$, $a_{2,2} = s_{2,2} = 131$ dan $a_{2,3} = s_{3,2} = 191$; partisipan p_3 memiliki $a_{3,1} = s_{1,3} = 147$, $a_{3,2} = s_{2,3} = 284$ dan $a_{3,3} = s_{3,3} = 49$; sedangkan partisipan p_4 memiliki $a_{4,1} = s_{1,4} = 162$, $a_{4,2} = s_{2,4} = 288$ dan $a_{4,3} = s_{3,4} = 225$. Selanjutnya rekonstruksi sub rahasia SK_1 menggunakan $(x_0, y_0) = (1,118), (x_1, y_1) = (2,86), (x_2, y_2) = (3,147), (x_3, y_3) = (4,162)$. Rekonstruksi sub rahasia SK_2 menggunakan $(x_0, y_0) = (1,29)$, $(x_1, y_1) = (2,131), (x_2, y_2) = (3,284), (x_3, y_3) = (4,288)$. Sedangkan rekonstruksi sub rahasia SK_3 menggunakan $(x_0, y_0) = (1,20)$, $(x_1, y_1) = (2,191), (x_2, y_2) = (3,49), (x_3, y_3) = (4,225)$.

Dengan interpolasi Lagrange:

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

maka diperoleh:

$$\begin{aligned} l_0(x) &= \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} \cdot \frac{x - x_3}{x_0 - x_3} \\ &= -\frac{1}{6}\left(x^3 - 9x^2 + 26x - 24\right) \end{aligned}$$

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

$$l_1(x) = \frac{x-x_0}{x_1-x_0}\cdot\frac{x-x_2}{x_1-x_2}\cdot\frac{x-x_3}{x_1-x_3}$$
$$= \frac{1}{2}\left(x^3 - 8x^2 + 19x - 12\right)$$

$$l_2(x) = \frac{x-x_0}{x_2-x_0}\cdot\frac{x-x_1}{x_2-x_1}\cdot\frac{x-x_3}{x_2-x_3}$$
$$= -\frac{1}{2}\left(x^3 - 7x^2 + 14x - 8\right)$$

$$l_3(x) = \frac{x-x_0}{x_3-x_0}\cdot\frac{x-x_1}{x_3-x_1}\cdot\frac{x-x_2}{x_3-x_2}$$
$$= \frac{1}{6}\left(x^3 - 6x^2 + 11x - 6\right)$$

Dengan $f(x) = \sum_{j=0}^{3} y_j \cdot l_j(x)$, maka persamaan *TS1, TS2, TS3* diperoleh:

$$TS_1 = 307.83x^3 + 185.5x^2 + 235.67x + 51$$

$$TS_2 = 297.67x^3 + 255.5x^2 + 320.83x + 178$$

$$TS_3 = 105.17x^3 + 205.5x^2 + 142.33x + 229$$

Sehingga diperoleh nilai subrahasia $SK_1 = 51,\ SK_2 = 178,\ SK_3 = 229$.

Selanjutnya subrahasia *SK1, SK2,* dan *SK3* akan digunakan untuk merekonstruksi kunci rahasia *K* dari persamaan polinomial $f(x) = K_2x^2 + K_1x + K_0$, dimana

$SK_1 = y_1 = f(1),\ SK_2 = y_2 = f(2),\ SK_3 = y_3 = f(3)$,

maka:

$$51 = K_2 + K_1 + K_0$$

$$178 = 4K_2 + 2K_1 + K_0$$

$$229 = 9K_2 + 3K_1 + K_0$$

dengan sistem persamaan linier (*SPL*), maka diperoleh kunci rahasia *K*, yaitu:

$$K = \{K_0, K_1, K_2\} = \{179, 241, 293\}$$

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

4.4 *Information Rate* Skema *3-STH*

Seperti telah dijelaskan pada Bab 2, i*nformation rate* dari skema pembagian rahasia yang dinotasikan dengan ρ, menurut Brickell dan Davenport (1991), dinyatakan dengan:

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

dimana *K* menunjukkan informasi rahasia yang didistribusikan kepada partisipan *P*, sedangkan *share* dari partisipan ke-*i* ditunjukkan oleh S_i, untuk $i = 1, 2,\ldots,n$.

Dari Contoh 4.7 telah diketahui kunci rahasia $K = \{K_0, K_1, K_2\}$, dimana $K_0 = 179$, $K_1 = 241$, dan $K_2 = 293$, diambil secara acak dari Z_{331}.

Ukuran *share* dari masing-masing S_i dari Tabel 4.2 adalah $|S_1| = 15$, $|S_2| = 15$, $|S_3| = 13$, $|S_4| = 14$, $|S_5| = 14$, $|S_6| = 12$, $|S_7| = 16$.

Maka *information rate* dari skema *3-STH* (Brickell & Davenport, 1991) adalah

$$\rho = \frac{\log_2 |K|}{\max_i \log_2 |S_i|} = \frac{\log_2 \left(2^9\right)^3}{\log_2 \left(2^9\right)^{16}} = \frac{3 \times \log_2 \left(2^9\right)}{16 \times \log_2 \left(2^9\right)} = \frac{3}{16}$$

Dari Gambar 4.1 dapat diketahui derajat dari masing-masing simpul yang dipandang sebagai partisipan p_i dari hipergraf *H* yaitu $p_1 = 4$, $p_2 = 4$, $p_3 = 6$, $p_4 = 5$, $p_5 = 2$, $p_6 = 3$ dan $p_7 = 0$, sehingga derajat terkecil dari hipergraf *H* adalah $d_{\min} = 2$.

Sehingga *information rate* skema *3-STH* dari Contoh 4.7 menurut Weng dan Juan (2005) adalah

$$\begin{aligned}\rho &= \max\{3/(C(n-1,2) - d_{\min} + 4), 3/(C(n-1,2)+1)\} \\ &= \max\{3/(C(6,2) - 2 + 4), 3/(C(6,2)+1)\} \\ &= \max\{3/17, 3/16\}\end{aligned}$$

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Hal ini sesuai dengan *information rate* yang diperoleh menurut Brickell dan Davenport (1997) yaitu $\rho = \frac{3}{16}$, sehingga perhitungan *information rate* dapat menggunakan rumus Brickell dan Davenport maupun Weng dan Juan.

Analisis perbandingan dari skema *3-SAH* dan skema *3-STH* akan dibahas pada bab berikutnya.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

BAB 5
ANALISIS PERBANDINGAN SKEMA *3-SAH* DENGAN *3-HTS*

Dalam Bab 3 dan Bab 4 telah dijelaskan mengenai skema pembagian rahasia struktur akses tipe I yang berdasarkan hipergraf *3-uniform*, yaitu skema 3-Struktur Akses Hipergraf (skema *3-SAH*) dan skema pembagian rahasia struktur akses tipe II yang berdasarkan hipergraf *3-uniform*, yaitu skema 3-Struktur Terlarang Hipergraf (skema *3-HTS*). Pada Bab ini akan dibahas tentang analisis perbandingan antara skema *3-SAH* dan skema *3-HTS*, meliputi persamaan dan perbedaan dari kedua skema, serta komplementasi antara kedua skema.

5.1 Persamaan Skema *3-SAH* dan Skema *3-STH*

Dari uraian Bab 3 dan Bab 4 diperoleh persamaan dari skema *3-SAH* dan skema *3-HTS*, yaitu:

a) Skema pembagian rahasia dikonstruksi berdasarkan hipergraf *3-uniform*, yaitu setiap hiperbusur dari suatu hipergraf H terdiri dari dari 3 simpul.

b) Himpunan simpul-simpul dari hipergraf H, direpresentasikan sebagai himpunan partisipan-partisipan dari skema pembagian rahasia yang dituliskan dengan $P = \{p_1, p_2, ..., p_n\}$, dimana himpunan dari semua subset dari P adalah 2^P.

c) Menggunakan suatu fungsi polinomial berderajat 2 dalam proses konstruksi skema pembagian rahasia. Hal ini disebabkan oleh proses konstruksi yang menggunakan skema Shamir-*Threshold*.

d) Proses menentukan *share* dari partisipan dalam konstruksi skema pembagian rahasia menggunakan suatu fungsi satu arah *hash* (g_{hash}).

e) Semua perhitungan dalam proses konstruksi dan rekonstruksi skemanya dilakukan atas lapangan Z_q, dimana q merupakan bilangan prima yang besar.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

f) *Information rate* (ρ) yang digunakan dari skema pembagian rahasia menurut Brickell dan Davenport (1991), dinyatakan dengan:

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

dimana K menunjukkan informasi rahasia yang didistribusikan kepada partisipan p_i, sedangkan *share* ke-i dari p_i untuk $i = 1, 2, ..., n$, ditunjukkan oleh S_i .

5.2 Perbedaan Skema *3-SAH* dengan Skema *3-STH*

Setelah melihat persamaan skema *3-SAH* dengan skema *3-STH* , berikut ini akan diuraikan perbedaan antara skema *3-SAH* dengan skema *3-STH* mulai dari tipe struktur akses yang digunakan, penentuan *share* dari skemanya, sifat struktur akses, pengambilan kunci rahasia *K*, sampai dengan *information rate* dari masing - masing skema. Uraian lengkap tentang perbedaan tersebut dapat dilihat pada Tabel 5.1.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Tabel 5.1 : Perbedaan Antara Skema *3-SAH* dan Skema *3-STH*

No	Skema *3-STH*	Skema *3-SAH*
1	Menggunakan struktur terlarang Δ sesuai tipe II menurut Sun dan Shieh (1997).	Menggunakan struktur akses Γ sesuai tipe I menurut Sun dan Shieh (1997).
2	Parameter dalam konstruksi skema: a) himpunan 3 partisipan yang bersesuaian dengan hiperbusur : $S = \{A : A \in E(H)\}$ b) Himpunan 3 partisipan yang diluar S : $R = \{A : A \notin E(H) \text{ dan } \lvert A \rvert = 3\}$. c) Struktur terlarang: $\Delta = \{A : A \subseteq P \text{ dan } \lvert A \rvert \le 2\} \cup \{A : A \in S\}$, d) Struktur akses-nya adalah: $\Gamma = 2^P \setminus \Delta = \{A : A \subseteq P \text{ dan } \lvert A \rvert \ge 4\} \cup \{A : A \in R\}$ e) Terdapat himpunan T yang memenuhi: $T = \{p_i : \exists p_j, p_k, p_l \in P \ni \{p_i, p_j, p_k\}, \{p_i, p_j, p_l\}, \{p_i, p_k, p_l\}, \{p_j, p_k, p_l\} \in E(H)$ dan $1 \le i \ne j \ne k \ne l \le n\}$	Parameter dalam konstruksi skema: a) *share* dari partisipan : $S = \{A : A \in E(H)\}$ b) Himpunan hiperbusur sebagai struktur akses minimal (Γ_0) , dengan $S \subseteq \Gamma_0$; $\Gamma_0 = \{A \in \Gamma : A' \not\subset A \ \forall A' \in \Gamma - \{A\}\}$. c) Struktur akses : $\Gamma = \{A \subseteq P \mid S \subseteq A \text{ for any } S \subseteq \Gamma_0\}$, d) Struktur terlarangnya adalah: $\Delta = 2^P \setminus \Gamma = \{A \subseteq P \mid S \not\subset A \ \forall S \subseteq \Gamma_0\}$ e) Tidak menggunakan himpunan T.
3	Sifat Struktur Terlarang: Struktur terlarang Δ memenuhi sifat monoton turun yaitu: $A \in \Delta$ dan $B \subseteq A \subseteq P \Rightarrow B \in \Delta$	Sifat Struktur Akses: Struktur akses Γ memenuhi sifat monoton naik yaitu: $A \in \Gamma$ dan $A \subseteq B \subseteq P \Rightarrow B \in \Gamma$
4	Pengambilan s*hare* : *Share* dari partisipan diambil berdasarkan hipergraf H, yaitu diambil dari 3 partisipan atau lebih yang tidak bersesuaian dengan hiperbusur.	Pengambilan s*hare* : *Share* dari partisipan diambil dari partisipan yang direpresentasikan oleh hipergraf H, yaitu 3 partisipan atau lebih yang bersesuaian dengan hiperbusur.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

No	Skema *3-STH*	Skema *3-SAH*
5	Pengambilan kunci rahasia yang digunakan: $K = \{K_0, K_1, K_2\}$, dimana K_0, K_1, K_2 diambil secara acak dari Z_q.	Pengambilan kunci rahasia yang digunakan: $K = \{K_0, K_1\}$, dimana K_0, K_1 diambil secara acak dari Z_q, sedangkan k_2 diambil sembarang dari Z_q.
6	Penggunaan persamaan polinomial: a) Dealer *D* mengkonstruksi $f(x) = K_2x^2 + K_1x + K_0$ b) $y_{(i,j)}$ dihitung dari *f(x)* yaitu: $y_{(i,j)} = f(i.n + j)$ untuk $1 \le i < j \le n$ c) $y_j = y_{(0,j)} = f(j)$ untuk $j = 1,2,3$.	Penggunaan persamaan polinomial: a) Dealer *D* mengkonstruksi $f(x) = k_2x^2 + K_1x + K_0$ b) $y_{(i,j)}$ dihitung dari *f(x)* yaitu: $y_{(i,j)} = f(i.n + j)$ untuk $1 \le i < j \le n$ c) Tidak menghitung y_j
7	Penggunaan *Subshare* dalam konstruksi: Dealer *D* mengkonstruksi 3 skema Shamir's *(4,n)-threshold*, yaitu TS_1, TS_2, TS_3 untuk menyembunyikan y_1, y_2, y_3, dengan ketentuan: $\forall(4,n) - TS_i$, y_i adalah sub-rahasia, $s_{i,1}, s_{i,2}, ..., s_{i,n}$ merupakan *n subshare*-nya	Penggunaan *Subshare* dalam konstruksi: Dealer *D* tidak menggunakan sub-rahasia y_1, y_2, y_3, sehingga tidak mempunyai *subshare* $s_{i,1}, s_{i,2}, ..., s_{i,n}$.
8	Ketentuan penyusunan *share:* Dealer *D* memilih sebanyak *n* bilangan acak atas Z_q yaitu: $r_1, r_2, ..., r_n$, untuk $1 \le i \le n$, *Share* p_i : $S_i = \langle a_{i,(1,2)}, a_{i,(1,3)}, ..., a_{i,(j,l)}, ..., a_{i,(n-1,n)}, a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4} \rangle$, $1 \le j < l \le n$ dengan syarat:	Ketentuan penyusunan *share*: Dealer *D* memilih sebanyak *n* bilangan acak atas Z_q yaitu: $r_1, r_2, ..., r_n$, untuk $1 \le i \le n$, *Share* p_i : $S_i = \langle a_{i,(1,2)}, a_{i,(1,3)}, ..., a_{i,(j,l)}, ..., a_{i,(n-1,n)}, r_i \rangle$, $1 \le j < l \le n$ dengan syarat:

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

No	Skema *3-STH*	Skema *3-SAH*
	$a_{i,(j,k)} = \begin{cases} y_{j,k} + g_{hash}(r_j \oplus r_k), \text{ jika } i \notin \{j,k\} \\ \text{dan } \{p_i, p_j, p_k\} \notin E(H); \\ \\ \text{kosong, untuk lainnya} \end{cases}$ $a_{i,j} = \begin{cases} s_{j,i}, \text{ jika } p_i \in T \text{ untuk } j = 1,2,3; \\ \text{kosong, untuk lainnya} \end{cases}$ $a_{i,4} = r_i$	$a_{i,(j,k)} = \begin{cases} y_{j,k} + g_{hash}(r_j \oplus r_k), \text{ jika} \\ \{p_i, p_j, p_k\} \in E(H); \\ \\ \text{kosong, untuk lainnya} \end{cases}$ Tidak terdapat $a_{i,j}$
9	*Information rate* dari skema akan memenuhi*:* $\rho = \max\{3/(C(n-1,2) - d_{\min} + 4), 3/(C(n-1,2)+1)\}$ dengan $d_{\min}$ merupakan derajat tekecil dari hipergraf *H*.	*Information rate* dari skema akan memenuhi*:* $\rho = \frac{2}{d_{\max} + 1}$, dengan $d_{\max}$ merupakan derajat terbesar dari hipergraf *H*.

5.3 Komplementasi Antara Skema *3-SAH* dan Skema *3-STH*

Pada konstruksi skema *3-SAH*, hiperbusur mewakili himpunan partisipan yang dapat mengakses kunci rahasia, sedangkan pada konstruksi skema *3-STH* himpunan partisipan yang mewakili hiperbusur justru tidak dapat mengakses kunci rahasia. Meskipun sekilas terlihat kedua skema saling komplemen satu dengan yang lain, tetapi kenyatannya tidak demikian. Teorema 3.2 dan Teorema 3.3 pada skema *3-SAH* menyatakan bahwa tidak semua himpunan partisipan yang terdiri dari lebih atau sama dengan 4 partisipan dapat mengakses kunci rahasia. Sedangkan pada Teorema 4.4 pada skema *3-STH* meyatakan bahwa setiap himpunan partisipan yang terdiri dari 4 atau lebih partisipan selalu dapat mengakses kunci rahasia.

Antara skema *3-SAH* dan skema *3-STH* tidak saling komplemen, artinya bahwa konstruksi dari skema *3-STH* bukan merupakan kebalikan atau komplemen dari skema *3-SAH*, begitu juga sebaliknya, konstruksi dari skema *3-SAH* bukan merupakan komplemen dari skema *3-SAH*.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

Sebagai ilustrasi, misalkan diambil contoh konstruksi pembagian rahasia yang sudah dibahas pada Bab 3 dan Bab 4. Seperti diketahui pada contoh dalam Bab 3 dan Bab 4, hipergraf yang digunakan berdasarkan pada Gambar 3.1 yang ditampilkan kembali pada Gambar 4.1.

Dari Contoh pada Bab 3 diperoleh:

$$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$$

$$E(H) = \Gamma_0 = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_2, p_6\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}, \{p_3, p_4, p_5\}, \{p_3, p_4, p_6\}, \{p_3, p_5, p_6\}\}$$

$$\Gamma = \{A \subseteq P \mid S \subseteq A \ \forall S \subseteq \Gamma_0\}$$

$$\Delta = 2^P \setminus \Gamma = \{A \subseteq P \mid S \not\subset A \ \forall S \subseteq \Gamma_0\}$$

Sedangkan dari Contoh pada Bab 4, diperoleh:

$$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7\}$$

$$S = \{A : A \in E(H)\} = \{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}, \{p_1, p_2, p_6\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}, \{p_3, p_4, p_5\}, \{p_3, p_4, p_6\}, \{p_3, p_5, p_6\}\}$$

$$R = \{A : A \notin E(H) \text{ dan } |A| = 3\}$$

$$\Delta = \{A : A \subseteq P \text{ dan } |A| \leq 2\} \cup \{A : A \in S\}$$

$$\Gamma = 2^P \setminus \Delta = \{A : A \subseteq P \text{ dan } |A| \geq 4\} \cup \{A : A \in R\}$$

Dilihat dari struktur aksesnya, Γ pada skema *3-STH* bukan komplemen dari Γ pada skema *3-SAH*. Misalnya diambil $A = \{p_1, p_2, p_3, p_4\}$; pada skema *3-STH*, himpunan partisipan $A = \{p_1, p_2, p_3, p_4\}$ dapat merekonstruksi kunci rahasia *K*. Pada skema *3-SAH*, himpunan partisipan $A = \{p_1, p_2, p_3, p_4\}$ juga dapat merekonstruksi kunci rahasia *K*. Artinya terdapat himpunan partisipan yang dapat merekonstruksi kunci rahasia *K* kedua skema, baik pada skema *3-SAH* maupun

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

pada skema *3-STH*. Sehingga dengan pengambilan contoh himpunan partisipan $A = \{p_1, p_2, p_3, p_4\}$, terjadi kontradiksi. Akibatnya skema *3-STH* bukan komplemen dari skema *3-SAH*.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

BAB 6
PENUTUP

Pada bab ini akan disampaikan kesimpulan dan saran yang diperoleh dari pembahasan skema pembagian rahasia *3-SAH* dan *3-STH* pada bab-bab sebelumnya.

6.1 Kesimpulan

Dari uraian tentang skema *3-SAH* dan skema *3-STH* pada bab-bab sebelumnya maka dapat diambil kesimpulan sebagai berikut:

1) Skema pembagian rahasia baik skema *3-SAH* dan *3-STH* merupakan suatu bentuk skema pembagian rahasia *non graphical* berdasarkan hipergraf *3-uniform*.
2) Konstruksi skema *3-SAH* dilihat dari simpul-simpul dalam hiperbusur dari hipergraf, sedangkan konstruksi skema *3-STH* dilihat dari himpunan simpul-simpul diluar hiperbusur.
3) Konstruksi skema *3-STH* bukan komplemen dari skema *3-SAH*.
4) Dilihat dari *information rate* ρ, skema *3-SAH* mempunyai nilai *information rate* yang lebih baik dari skema *3-STH*.
5) Dilihat dari proses konstruksi dan rekonstruksinya, struktur skema *3-SAH* lebih sederhana dari struktur skema *3-STH*.

6.2 Saran

Setelah melihat analisis perbandingan skema *3-SAH* dan skema *3-STH* , serta berdasarkan pengkajian yang telah dilakukan, terdapat saran sebagai berikut:

Perlu pengkajian lebih lanjut untuk memperoleh bentuk umum dari skema pembagian rahasia yang berdasarkan hipergraf baik untuk stuktur akses maupun struktur terlarang.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

DAFTAR PUSTAKA

Blundo, C., De Santis, A., Gargano, L ., dan Vaccaro, U. (1993). On The Information rate of Secret Sharing Schemes. *Proc. of Crypto'92, Lecture Notes in Computer Science*, 740, Springer Verlag, 148-167.

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.

Csirmaz, László. (1997). The Size of a Share Must Be Large. *Journal of Cryptology*, 10, 223-231.

Garnier, Rowan., and Taylor, John. (2002). *Discret Mathematics for New Technology* (2nd ed.). Philadelpia: IOP Publishing,

Goldreich, Oded. (2004). *Foundations of Criptography* (*Basic Technique*). Cambridege University Press.

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

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

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

Rosen, Kenneth H. (2000). *Handbook of Discrete and Combinatorial Mathematics*. New York: CRC Press.

Schneier, Bruce. (1986.) *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C.* John Wiley & Son Inc.,

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

Stalings, William. Cryptography and Network Security. Principle and Practice. Pearson Education, 2003.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.

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

Wang, Yi-Chun., and Juan, Justie Su-tzu. (2007). A Perfect Secret Sharing Scheme for r-Uniform Hypergraph-Based Access Structures. *Proceeding of The 24rd Workshop on Combinatorial Mathematics and Computation Theory*, 28-34.

Weng, Yu-fen and Juan, Justie Su-tzu. (2005). A Skilled Secret Sharing Scheme for r-Uniform Hypergraph-Based Prohibited Structures. *Proceeding of The 23rd Workshop on Combinatorial Mathematics and Computation Theory*, 336-344.

Analisis perbandingan..., I Ketut Tri Martana, FMIPA UI, 2010.