UNIVERSITAS INDONESIA

PENGARUH TRANSFORMASI HIMPUNAN PEMBANGKIT PADA FUNGSI *HASH* DARI GRAF EKSPANDER LUBOTZKY-PHILLIPS-SARNAK

TESIS

PETER JOHN
1006734571

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI MATEMATIKA
DEPOK
JANUARI 2012

UNIVERSITAS INDONESIA

PENGARUH TRANSFORMASI HIMPUNAN PEMBANGKIT PADA FUNGSI *HASH* DARI GRAF EKSPANDER LUBOTZKY-PHILLIPS-SARNAK

TESIS
Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Sains

PETER JOHN
1006734571

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI MATEMATIKA
DEPOK
JANUARI 2012

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	**: Peter John**
NPM	**: 1006734571**
Tanda Tangan	**:** 
Tanggal	**: Januari 2012**

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :

Nama	: Peter John
NPM	: 1006734571
Program Studi	: Matematika
Judul Tesis	: Pengaruh Transformasi Himpunan Pembangkit pada Fungsi *Hash* dari Graf Ekspander Lubotzky-Phillips-Sarnak.

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

DEWAN PENGUJI

Pembimbing I : Dr. Kiki A. Sugeng ( )

Pembimbing II: Dra. Nora Hariadi, M.Si ( )

Penguji : Prof. Dr. Djati Kerami ( )

Penguji : Dr. rer. nat. Hendri Murfi, M.Kom. ( )

Penguji : Dr. Al Haji Akbar B., M.Sc. ( )

Ditetapkan di : Depok

Tanggal : 12 Januari 2012

KATA PENGANTAR

Puji syukur senantiasa penulis panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya, penulisan tesis ini dapat diselesaikan. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk meraih gelar Magister Sains di Departemen Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Indonesia. Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai penyusunan tugas akhir ini, sangatlah sulit bagi penulis untuk menyelesaikan tesis ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Ibu Kiki A. Sugeng dan Ibu Nora Hariadi selaku pembimbing tugas akhir yang telah meluangkan waktunya untuk memberikan bimbingan, motivasi, saran, pengarahan dan kemudahan lainnya dengan sangat sabar sehingga tesis ini dapat diselesaikan dengan baik.
2. Bapak Djati Kerami selaku ketua program studi Magister Matematika UI dan Bapak Hengki Tasman selaku pembimbing akademis penulis, yang selalu membimbing dan memotivasi penulis untuk terus berusaha menyelesaikan tugas-tugas yang dibebankan pada saya selama proses perkuliahan.
3. Seluruh staf pengajar Departemen Matematika UI yang telah bersedia untuk meluangkan waktunya untuk membagi ilmu dan berdiskusi dengan penulis selama masa perkuliahan penulis.
4. Istri tercinta, Fransiska Liminda dan putri tercinta, Dharma Preuchia, yang selalu memberikan dukungan kepada penulis untuk memperoleh hasil terbaik selama proses perkuliahan dan penyelesaian tesis.
5. Seluruh anggota keluarga penulis yang selalu membantu, memberikan dukungan, dan selalu menemani hari-hari penulis dengan canda dan tawa.
6. Seluruh karyawan Departemen Matematika yang telah banyak memberikan bantuan dalam pengurusan administrasi.
7. Teman-teman seperjuangan: Pak Ketua Uun, Bu Desti, Kak Feni, Nurma, Rifkos, Bu Debby, Kak Dewi, Mbak Murtiningrum, Pak Haryono, Bu Rina, Pak Iwan, Pak Martin, Kak Iif, Bu Mia, Pak Ayin, Pak Huda, Pak Aziz.

8. Teman-teman Magister Matematika angkatan 2010 lainnya: Mbak Rida, Mbak Risda, Mbak Siti, Mbak Fathin, Mbak Lisa, Mbak Lia, Mbak Titi, Bu Tri, Bu Endang, Bu Sagita, Pak Umar, Pak Subian, Pak Supri, Pak Endaryono, Pak Bob, Pak Tarhadi, Pak Sigit.
9. Serta untuk semua pihak yang tidak dapat disebutkan satu-persatu yang telah membantu penulis dalam proses pembuatan dan penyelesaian tesis ini.

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan tesis ini. Untuk itu, penulis mengharapkan segala kritik dan saran yang membangun dari para pembaca untuk menyempurnakan tesis ini.

Akhir kata, penulis memohon maaf atas segala kesalahan dan kekurangan dalam tesis ini. Semoga tesis ini dapat berguna bagi siapa saja yang mengkajinya, serta dapat dikembangkan dan disempurnakan agar lebih bermanfaat untuk kepentingan orang banyak.

Depok, Januari 2012

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama	: Peter John
NPM	: 1006734571
Program Studi	: Matematika
Departemen	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam
Jenis karya	: Tesis

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

Pengaruh Transformasi Himpunan Pembangkit Pada Fungsi *Hash* Dari Graf Ekspander Lubotzky-Phillips-Sarnak

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

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada tanggal : Januari 2012

Yang menyatakan

(Peter John)

Abstrak

Nama : Peter John
Program Studi : Matematika
Judul : Pengaruh Transformasi Himpunan Pembangkit pada Fungsi *Hash* dari Graf Ekspander Lubotzky-Phillips-Sarnak

Ketahanan tumbukan adalah salah satu sifat penting dari suatu fungsi *hash*. Suatu fungsi *hash* f dikatakan mempunyai sifat ketahanan tumbukan jika diberikan suatu nilai *hash* $f(m)$ maka sulit menemukan suatu anggota domain m' yang mempunyai nilai *hash* $f(m')$, dengan $f(m') = f(m)$ tetapi $m' \neq m$. Pada tahun 2008, Tillich-Zemor membuktikan bahwa fungsi *hash* yang dibangun dari graf ekspander LPS yang dikonstruksi oleh Charles-Goren-Lauter (2007) tidak memenuhi sifat ketahanan tumbukan. Untuk menghindari hal tersebut dilakukan perbaikan dengan melakukan transformasi himpunan pembangkit S_p dari fungsi *hash* menjadi himpunan pembangkit ${S_p}^2$. Pada tesis ini dilakukan pembuktian secara matematis bahwa Teorema Tillich-Zemor tidak dapat digunakan pada hasil transformasi fungsi *hash* yang dibangun dengan himpunan pembangkit ${S_p}^2$.

Kata kunci : fungsi *hash*, graf ekspander LPS, Teorema Tillich-Zemor, ketahanan tumbukan.
xi+29 halaman; 3 tabel; 3 gambar
Daftar Pustaka : 12 (1922 – 2010)

Abstract

Name : Peter John
Departement : Matematika
Title : The Influence of Transformation of Generator Set in Hash Function from Lubotzky-Phillips-Sarnak Expander Graph

Collision resistant is one of important properties of a hash function. Hash function f is called to satisfied the collision resistant if given a hash value $f(m)$ then it will difficult to find another m' from domain of f which has a hash value $f(m')$, where $f(m') = f(m)$ and $m' \neq m$. In 2008, Tillich-Zemor proved that the hash function of LPS expander graph constructed by Charles-Goren-Lauter (2007) does not satisfies collision resistant. To avoid that, the improvement done by transforming the generator set S_p of hash function to be generator set ${S_p}^2$. This thesis is done a mathematically prove that the Tillich-Zemor Theorem cannot be applied in the transformation of the hash function constructed by generator set ${S_p}^2$.

Keywords : hash function, LPS expander graph, Tillich-Zemor Theorem, collision resistant.
xi+29 pages; 3 tables; 3 figures
Bibliography : 12 (1922 – 2010)

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB 1

PENDAHULUAN

1.1. Latar Belakang

Pada abad XX, kriptografi menjadi salah satu alat penting untuk militer dalam perang dunia. Saat ini, kriptografi telah digunakan oleh sebagian besar orang untuk berbagai macam kegiatan, seperti surat elektronik, tranksaksi secara *online*. Menurut Menezes dkk. (1996) dalam bukunya yang berjudul "*Handbook of Applied Cryptography*", Menezes menyatakan kriptografi adalah studi mengenai teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan (*confidentiality*), keutuhan data (*data integrity*), otentikasi data (*data authentication*), dan otentikasi asal data (*data origin authentication*). Tujuan utama dari kriptografi adalah melindungi data dari pencurian atau pengubahan oleh *malicious adversaries.* Salah satu perangkat dasar dalam kriptografi adalah fungsi *hash*. Penggunaan utama dari fungsi *hash* adalah sebagai tanda tangan digital (*digital signature*) dan kode otentikasi pesan (*message authentication codes*), namun saat ini fungsi *hash* telah digunakan di banyak aplikasi yang memerlukan sifat-sifat tertentu. Sifat yang paling penting adalah ketahanan prapeta (*preimage resistance*) dan ketahanan tumbukan (*collision resistance*).

Dalam perkembangannya, fungsi *hash* telah dikonstruksikan dengan berbagai cara, antara lain konstruksi Merkle-Damgård, konstruksi Charles-Goren-Lauter. Konstruksi Merkle-Damgård adalah konstruksi yang diusulkan secara terpisah oleh Merkle pada tahun 1979 dan Damgård pada tahun 1989. (Petit, 2009)

Konstruksi Charles-Goren-Lauter (CGL) adalah suatu konstruksi fungsi *hash* dari graf ekspander. Charles-Goren-Lauter (2007) menggunakan keluarga graf Ramanujan yang dikonstruksi berturut-turut oleh Lubotzky-Phillips-Sarnak (1988) dan Pizer (1990). Gagasan yang ditawarkan pada konstruksi ini adalah penggunaan graf ekspander untuk menghasilkan fungsi *hash* yang memiliki ketahanan tumbukan, karena pesan yang dijadikan prapeta akan menjadi penentu lintasan (tanpa berjalan mundur) yang akan dilalui pada graf ekspander yang digunakan, dan yang menjadi petanya adalah simpul (*vertex*) pada akhir lintasan.

Petit (2009) menyatakan bahwa semua serangan yang dilakukan pada konstruksi yang menggunakan keluarga graf Ramanujan dari Pizer tidak menghasilkan tumbukan secara efektif. Namun, Tillich-Zemor (2008) menunjukkan bahwa serangan terhadap konstruksi CGL yang menggunakan keluarga graf Ramanujan dari Lubotzky-Phillips-Sarnak dapat menghasilkan tumbukan, dan Petit (2009) menunjukkan bahwa serangan prapeta terhadap konstruksi ini juga dapat menghasilkan tumbukan. Untuk mengatasi masalah ini disarankan untuk mengubah himpunan pembangkit dari fungsi *hash* dari S menjadi S^2, dengan S^2 adalah himpunan yang anggota-anggotanya merupakan kuadrat dari anggota-anggota di S. (Tillich-Zemor, 2008)

1.2. Masalah penelitian

Permasalahan yang dibahas pada tesis ini adalah pengaruh transformasi himpunan pembangkit dari fungsi *hash* dan sifat-sifat yang dipertahankan dari hasil transformasi tersebut.

1.3. Tujuan Penelitian

Penelitian ini bertujuan untuk meneliti pengaruh transformasi himpunan pembangkit S dari fungsi *hash* menjadi S^2 terhadap serangan yang dilakukan oleh Tillich-Zemor (2008) dan meneliti sifat-sifat yang dipertahankan dari hasil transformasi tersebut.

1.4. Metode Penelitian

Metode penyelesaian masalah yang digunakan dalam penelitian ini adalah studi literatur dengan mempelajari berbagai buku dan jurnal yang terkait dengan topik penelitian dan pengkajian terhadap pengaruh transformasi himpunan pembangkit terhadap keamanan fungsi *hash* yang dibangun.

BAB 2

LANDASAN TEORI

Pada bab ini akan dijelaskan mengenai hal-hal yang menjadi teori dasar dari penelitian yang dilakukan yang dibagi menjadi 2 subbab yaitu subbab pertama yang berjudul Teori Grup, Teori Graf dan Fungsi *Hash*, dan subbab kedua yang berjudul *Quaternion*. Subbab pertama akan menjelaskan tentang beberapa teori dasar dari teori grup, teori dasar dari teori graf, graf Cayley, graf ekspander, dan fungsi *Hash*. Subbab kedua akan menjelaskan tentang pengertian dasar *quaternion* dan beberapa karakteristik *quaternion* yang dibutuhkan pada penelitian ini.

2.1. Teori Grup, Teori Graf dan Fungsi *Hash*

2.1.1. Teori Grup

Subbab ini membahas tentang beberapa teori dasar pada teori grup yang akan digunakan pada bab-bab selanjutnya.

Definisi 2.1. (Hungerford, 1973) Suatu **grup** adalah suatu himpunan tak kosong G bersama dengan operator biner $*$ yang memenuhi sifat-sifat berikut.

1. (Asosiatif) Untuk setiap $a, b, c \in G$ memenuhi $(a * b) * c = a * (b * c)$
2. (Identitas) Terdapat $e \in G$ sedemikian sehingga $a * e = e * a = a$, untuk setiap $a \in G$
3. (Invers) Untuk setiap $a \in G$, terdapat $a^{-1} \in G$ sedemikian sehingga $a * a^{-1} = a^{-1} * a = e$.

Contoh 2.1: Misalkan G adalah himpunan yang beranggotakan matriks real berukuran 2×2 dengan determinan tak nol. Maka $(G,\times)$ membentuk grup, dengan operasi biner $\times$ adalah perkalian antara dua buah matriks.

Jika suatu grup G memenuhi sifat komutatif pada operasi binernya maka disebut sebagai grup komutatif (*Abelian group*). Suatu grup dikatakan berhingga jika banyak anggota dari grup tersebut berhingga.

Jika diberikan suatu grup G dan $S \subseteq G$, maka S^{-1} adalah himpunan yang anggotanya merupakan invers dari anggota-anggota S. Dengan perkataan lain $S^{-1} = \{s^{-1} : s \in S\}$.

Definisi 2.2. (Petit, 2009) Misalkan G suatu grup dan $S \subseteq G$. S disebut **himpunan simetris** (*symmetric set*) jika $S = S^{-1}$.

Contoh 2.2: Misalkan $G = \mathbf{Z}_6$ adalah grup dengan operasi penjumlahan modulo 6. Misalkan pula $S = \{2, 4\} \subseteq G$ maka $S^{-1} = S$.

Definisi 2.3. (Hungerford, 1993) Misalkan G suatu grup dan H himpunan bagian yang tak kosong dari G yang memenuhi sifat tertutup terhadap operasi $*$. Jika H membentuk grup dengan operasi $*$ maka H disebut **subgrup** pada G dan dinotasikan sebagai $H < G$.

Contoh 2.3: Misalkan G adalah grup yang didefinisikan pada Contoh 2.2 dan himpunan $H = \{0,2,4\}$, maka $H < G$.

Misalkan G suatu grup dengan operasi $*$, $H < G$ dan $a \in G$ maka himpunan $Ha = \{h * a : h \in H\}$ disebut koset kanan dari H di G dan himpunan $aH = \{a * h : h \in H\}$ disebut koset kiri dari H di G. Banyaknya koset kiri berbeda dari H di G dinotasikan sebagai $[G:H]$. (Hungerford, 1993)

Teorema 2.1. (*Lagrange*)(Hungerford, 1993) Misalkan G suatu grup berhingga. Jika $H < G$ maka $|G| = [G:H]|H|$.

Definisi 2.4. (Hungerford, 1993) Misalkan G suatu grup dan $N < G$. Jika $aN = Na$, untuk setiap $a \in G$ maka N disebut **subgrup normal** dari G dan dinotasikan sebagai $N \lhd G$.

Contoh 2.4: Misalkan G adalah himpunan matriks non singular berukuran 2×2 bersama dengan operasi perkalian matriks, maka G membentuk grup. Misalkan $N = \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} : \lambda \in \mathbf{R} - \{0\} \right\}$, maka $N \lhd G$.

Teorema 2.2. (Hungerford, 1993) Jika $N \lhd G$ dan G/N adalah himpunan semua koset kiri dari N di G, maka G/N adalah grup berorder $[G:N]$ dengan operasi biner yang didefinisikan sebagai $(aN)(bN) = abN$.

Grup G/N yang dijelaskan pada Teorema 2.2 disebut sebagai grup kuosien (*quotient group*) dari G oleh N. (Hungerford, 1993)

Definisi 2.5. (Hungerford, 1993) Suatu **lapangan** (*field*) adalah himpunan tak kosong F bersama dengan dua operasi biner, $+$ dan $*$, sedemikian sehingga

(i) $(F, +)$ merupakan grup komutatif

(ii) $(F - \{0\}, *)$ merupakan grup komutatif.

(iii) $a * (b + c) = (a * b) + (a * c)$ dan $(b + c) * a = (b * a) + (c * a)$ untuk setiap $a, b, c \in F$.

Contoh 2.5: Misalkan $F = \left\{M = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbf{R}\right\}$. Maka himpunan F bersama dengan operasi penjumlahan dan perkalian matriks merupakan lapangan.

Lapangan hingga adalah lapangan yang banyak anggotanya berhingga.

Selanjutnya akan dibahas beberapa teori dasar pada teori graf yang digunakan pada bab-bab selanjutnya.

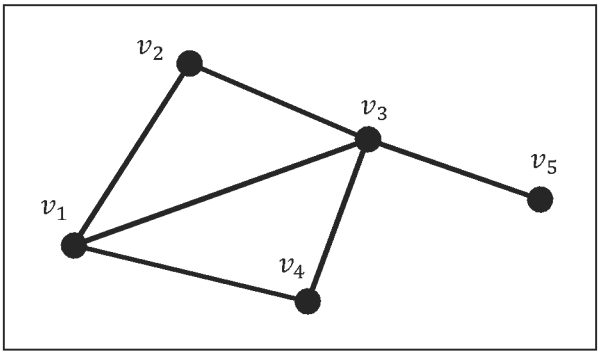
2.1.2. Teori Graf

Subbab ini membahas tentang beberapa teori dasar pada teori graf, pengertian graf Cayley dan graf ekspander yang akan digunakan pada bab-bab selanjutnya.

Definisi 2.6. (Rosen, 2007) Suatu **graf sederhana** $G = (V, E)$ mengandung himpunan V, himpunan simpul yang tak kosong, dan himpunan E suatu himpunan pasangan tak terurut dari elemen-elemen di V yang disebut himpunan busur.

Contoh 2.6: Misalkan $V = \{v_1, v_2, v_3, v_4, v_5\}$ dan $E = \{(v_1, v_2), (v_1, v_3), (v_2, v_3), (v_3, v_4), (v_3, v_5), (v_4, v_1)\}$ maka $G = (V, E)$ adalah suatu graf sederhana seperti yang terlihat pada Gambar 2.1.

Ukuran suatu graf G adalah banyaknya simpul pada graf G. Dengan demikian ukuran graf G pada Contoh 2.6 adalah 5 karena graf G memiliki 5 simpul.



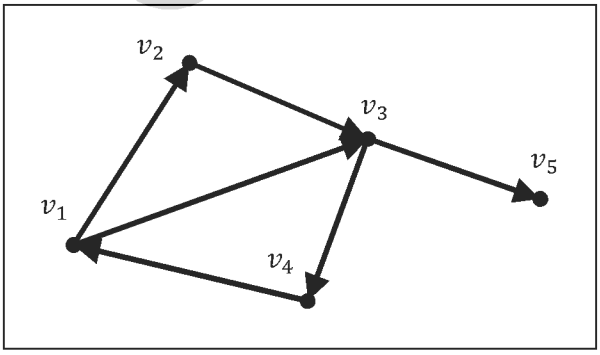
Gambar 2.1. Graf sederhana $\boldsymbol{G(V,E)}$, $\boldsymbol{V = \{v_1, v_2, v_3, v_4, v_5\}}$, $\boldsymbol{E = \{(v_1, v_2), (v_1, v_3), (v_1, v_4), (v_2, v_3), (v_3, v_4), (v_3, v_5)\}}$.

Definisi 2.7. (Rosen, 2007) Dua simpul u dan v pada graf sederhana G dikatakan **bertetangga** (*adjacent*) jika (u, v) merupakan busur pada G. Jika $e = (u, v)$ ada di G maka busur e dikatakan **terhubung** (*incident*) dengan simpul u dan v.

Contoh 2.7: Berdasarkan Contoh 2.6, maka simpul v_1 dan v_2 dikatakan bertetangga karena (v_1, v_2) merupakan busur di G dan busur (v_1, v_2) dikatakan terhubung dengan simpul v_1 dan simpul v_2.

Definisi 2.8. (Rosen, 2007) Suatu **graf berarah** $G = (V, E)$ mengandung himpunan V, himpunan simpul yang tak kosong, dan himpunan E suatu himpunan pasangan terurut dari elemen-elemen di V yang disebut himpunan busur berarah.

Contoh 2.8: Misalkan $V = \{v_1, v_2, v_3, v_4, v_5\}$ dan $E = \{(v_1, v_2), (v_1, v_3), (v_2, v_3), (v_3, v_4), (v_3, v_5), (v_4, v_1)\}$, dan E merupakan himpunan busur berarah maka $G = (V, E)$ adalah suatu graf berarah seperti yang terlihat pada Gambar 2.2.



Gambar 2.2. Graf berarah $\boldsymbol{G(V,E)}$, $\boldsymbol{V = \{v_1, v_2, v_3, v_4, v_5\}}$, $\boldsymbol{E = \{(v_1, v_2), (v_1, v_3), (v_2, v_3), (v_3, v_4), (v_3, v_5), (v_4, v_1)\}}$.

Definisi 2.9. (Rosen, 2007) **Derajat** dari suatu simpul v pada graf sederhana G adalah banyaknya busur di G yang terhubung dengan simpul v.

Contoh 2.9: Simpul v_1 pada Contoh 2.6 mempunyai derajat 3.

Suatu graf sederhana disebut k-regular jika setiap simpul pada graf tersebut mempunyai derajat k.

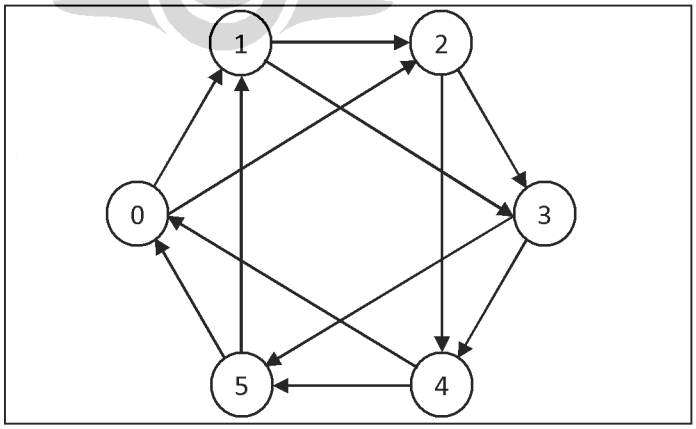
Definisi 2.10. (Rosen, 2007) Suatu **lintasan** (*path*) dengan panjang n dari simpul u_0 ke simpul u_n adalah barisan busur $(u_0, u_1), (u_1, u_2), \ldots, (u_{n-1}, u_n)$. Suatu lintasan disebut **sirkuit** (*cycle*) jika simpul $u_0 = u_n$.

Contoh 2.10: Barisan busur $(v_1, v_2), (v_2, v_3), (v_3, v_5)$ pada Contoh 2.6 merupakan lintasan dengan panjang 3 dari simpul v_1 ke v_5. Barisan busur $(v_1, v_2), (v_2, v_3), (v_3, v_4), (v_4, v_1)$ pada Contoh 2.6 merupakan sirkuit dengan panjang 4.

Definisi 2.11. (Davidoff, 2003) Panjang sirkuit yang terpendek dari suatu graf disebut ***girth***.

Contoh 2.11: *Girth* dari graf pada Gambar 2.1 adalah 3.

Definisi 2.12. (Davidoff, 2003) Misalkan $(G,*)$ suatu grup, himpunan V mempunyai hubungan korespondensi satu-satu dengan G, $S \subseteq G$, dan E adalah himpunan pasangan berurut (v_g, v_h) dengan $h = g * s$, untuk $g, h \in G$, $s \in S$. Maka graf dengan himpunan simpul V dan himpunan busur E disebut sebagai **graf Cayley** yang dinotasikan sebagai $C_{G,S}(V, E)$.



Gambar 2.3. Graf Cayley yang dibangun dari $(\mathbf{Z_6}, +)$ dan $\boldsymbol{S} = \{1, 2\}$.

Gambar 2.3 menggambarkan suatu graf Cayley yang dibangun dari grup $(\mathbf{Z}_6, +)$ dan $S = \{1, 2\}$.

Untuk membangun graf pada Gambar 2.3, mula-mula dipilih himpunan simpul $V = \{0,1,2,3,4,5\}$ karena himpunan V mempunyai hubungan korespondensi satu-satu dengan $\mathbf{Z}_6$, dan untuk menghasilkan himpunan busur maka dicari pasangan (v, w), dengan $w = v + s$ untuk suatu $s \in S$ sehingga akan diperoleh $E = \{(0,1), (0,2), (1,2), (1,3), (2,3), (2,4), (3,4), (3,5), (4,5), (4,0), (5,1), (5,2)\}$.

Misalkan $G(V, E)$ suatu graf sederhana yang mempunyai n simpul dan $H \subseteq V$. Batas busur (*edge boundary*) dari H adalah himpunan busur yang menghubungkan simpul-simpul H dengan $\overline{H}$ (komplemen dari H). Batas busur dari H dinotasikan sebagai ∂H. Parameter ekspansi (*expansion parameter*) dari suatu graf dinotasikan sebagai $h(G)$, didefinisikan sebagai

$$h(G) = \min_{\left\{H:|H|\leq\frac{n}{2}\right\}} \frac{|\partial H|}{|H|}.$$

Definisi 2.13. (Linial, 2003) **Keluarga graf ekspander** $\{G_i\}$, $i \in \mathbf{N}$ adalah koleksi graf yang memenuhi sifat-sifat berikut:

1. Graf G_i adalah graf k-regular dengan ukuran n_i. $\{n_i\}$ membentuk barisan monoton naik yang tidak tumbuh dengan cepat. Salah satu kriteria barisan yang memenuhi sifat monoton naik yang tidak tumbuh dengan cepat adalah $n_{i+1} < {n_i}^2$
2. $h(G_i) \geq \varepsilon > 0$, untuk setiap i.

Contoh 2.12: Keluarga dari graf-graf yang berukuran p, untuk semua p bilangan prima. Himpunan simpul $V_p = \mathbf{Z}_p$ dan setiap graf merupakan graf 3-regular. Setiap simpul x bertetangga dengan $x - 1, x + 1$, dan x^{-1}. Maka keluarga graf ini merupakan keluarga graf ekspander. (Lubotsky dkk., 1988).

Pada bagian selanjutnya akan menjelaskan tentang teori dasar fungsi *hash*.

2.1.3. Fungsi *Hash*

Definisi 2.14. (Charles, 2007) Untaian adalah rangkaian simbol-simbol. Diberikan suatu himpunan A^* yang beranggotakan untaian-untaian dengan panjang sembarang dan himpunan A^m yang beranggotakan himpunan untaian-untaian dengan panjang m. Maka **fungsi *hash* kriptografis** f adalah fungsi yang memetakan dari A^* ke A^m dan mudah untuk dihitung.

Berikut ini adalah dua sifat yang harus terpenuhi dari suatu fungsi *hash* kritografis untuk dikatakan aman, yaitu:

1. Ketahanan prapeta (*preimage resistance*)
   Ketahanan prapeta akan terpenuhi jika diberikan suatu nilai fungsi *hash*, maka akan sulit secara komputasi untuk menemukan nilai prapeta yang bisa menghasilkan nilai fungsi *hash* tersebut.
2. Ketahanan tumbukan (*collision resistance*)
   Ketahanan tumbukan akan terpenuhi jika secara komputasi sulit untuk menemukan dua nilai prapeta berbeda yang memiliki nilai fungsi *hash* yang sama.

Menurut Charles-Goren-Lauter (2007), permasalahan untuk menghasilkan suatu tumbukan dari suatu serangan terhadap fungsi *hash* dari graf ekspander sama artinya dengan permasalahan untuk mencari dua lintasan berbeda untuk dua simpul dari graf ekspander. Pada penelitian ini sifat fungsi *hash* kritografis yang akan dibahas adalah sifat ketahanan tumbukan.

2.2. *Quaternion*

Definisi 2.15. (Dickson, 1922) Misalkan F adalah suatu lapangan dan himpunan $H(F)$ adalah himpunan semua objek yang berbentuk $a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k}$, dengan $a_0, a_1, a_2, a_3 \in F$ dan $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ memenuhi relasi berikut

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1,\ \boldsymbol{ij} = \boldsymbol{k} = -\boldsymbol{ji}, \boldsymbol{jk} = \boldsymbol{i} = -\boldsymbol{kj}, \boldsymbol{ki} = \boldsymbol{j} = -\boldsymbol{ik},$$

maka $H(F)$ disebut himpunan ***quaternion***.

Contoh 2.13: Misalkan F suatu lapangan dengan himpunan tak kosong $\{0,1\}$ bersama operasi penjumlahan modulo 2 dan operasi perkalian. Maka

$$H(F) = \{0,1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}, 1+\boldsymbol{i}, 1+\boldsymbol{j}, 1+\boldsymbol{k}, \boldsymbol{i}+\boldsymbol{j}, \boldsymbol{i}+\boldsymbol{k}, \boldsymbol{j}+\boldsymbol{k}, 1+\boldsymbol{i}+\boldsymbol{j},$$
$$1+\boldsymbol{i}+\boldsymbol{k}, 1+\boldsymbol{j}+\boldsymbol{k}, \boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}, 1+\boldsymbol{i}+\boldsymbol{j}+\boldsymbol{k}\}$$

merupakan suatu himpunan *quaternion*.

Jika $q \in H(F)$ maka $q = a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k}$, maka konjugat dari q adalah $\bar{q} = a_0 - a_1\boldsymbol{i} - a_2\boldsymbol{j} - a_3\boldsymbol{k}$. Norma (*norm*) dari q adalah

$$N(q) = q\bar{q} = {a_0}^2 + {a_1}^2 + {a_2}^2 + {a_3}^2.$$

Operasi perkalian pada dua anggota $H(F)$, $q = a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k}$ dan $r = b_0 + b_1\boldsymbol{i} + b_2\boldsymbol{j} + b_3\boldsymbol{k}$ yang dinotasikan sebagai $q \times r$ didefinisikan sebagai

$$q \times r = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)\boldsymbol{i}$$
$$+(a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)\boldsymbol{j} + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)\boldsymbol{k}.$$

Operasi $\times$ pada $H(F)$ memenuhi hukum asosiatif. *Quaternion* q juga sering ditulis dalam bentuk 4-*tuple* (a_0, a_1, a_2, a_3). Suatu *quaternion* q dikatakan integral jika $a_0, a_1, a_2, a_3 \in \mathbf{Z}$. Jika q, r, dan s adalah integral *quaternion* sedemikian sehingga $q = r \times s$, maka q dikatakan memiliki s sebagai pembagi kanan (*right-hand divisor*) dan r sebagai pembagi kiri (*left-hand divisor*). Suatu integral *quaternion* yang nilai normanya 1 maka disebut sebagai *quaternion unit*. Hanya ada 8 *quaternion unit* pada integral *quaternion* yaitu $1, -1, \boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{j}, \boldsymbol{k}$, dan $-\boldsymbol{k}$. Suatu *quaternion* q dikatakan terhubung (*associated*) dengan r jika r adalah hasil kali q dengan suatu *quaternion unit*. Suatu integral *quaternion* q dikatakan ganjil jika $N(q) \equiv 1 \pmod 2$. (Dickson, 1922)

Teorema 2.3. (Dickson, 1922) Jika c adalah sebarang *quaternion* ganjil dan $N(c) = \prod_{i=1}^{m} p_i$, dengan p_i adalah faktor prima dari $N(c)$, maka $c = \prod_{i=1}^{m} q_i$, dengan $N(q_i) = p_i$, untuk $i = 1, 2, \ldots, m$.

Untuk mengetahui banyaknya integral *quaternion* yang mempunyai norma yang sama besar dapat digunakan Teorema Jacobi yang dikenal sebagai Teorema *Jacobi's four square*.

Teorema 2.4. (***Jacobi's four-square***)(Hirschhorn, 1987) Jika (a, b, c, d) adalah 4-*tuple* yang memenuhi persamaan

$$a^2 + b^2 + c^2 + d^2 = n \tag{2.1}$$

maka

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d$$

dengan $r_4(n)$ adalah banyaknya 4-*tuple* berbeda yang memenuhi Persamaan (2.1).

Contoh 2.14: Jika diberikan $p = 5$, maka menurut Teorema *Jacobi's four-square* ada sebanyak $8(5 + 1) = 48$ integral *quaternion* berbeda dengan norma sebesar p yang tercantum pada Tabel 2.1.

Tabel 2.1. Himpunan *quaternion-quaternion* bernorma **5**.

$(1,2,0,0)$	$(-2,1,0,0)$	$(0,0,1,-2)$	$(0,0,2,1)$
$(-1,-2,0,0)$	$(2,-1,0,0)$	$(0,0,-1,2)$	$(0,0,-2,-1)$
$(1,0,2,0)$	$(0,1,0,2)$	$(-2,0,1,0)$	$(0,-2,0,1)$
$(-1,0,-2,0)$	$(0,-1,0,-2)$	$(2,0,-1,0)$	$(0,2,0,-1)$
$(1,0,0,2)$	$(0,1,-2,0)$	$(0,2,1,0)$	$(-2,0,0,1)$
$(-1,0,0,-2)$	$(0,-1,2,0)$	$(0,-2,-1,0)$	$(2,0,0,-1)$
$(1,-2,0,0)$	$(2,1,0,0)$	$(0,0,1,2)$	$(0,0,-2,1)$
$(-1,2,0,0)$	$(-2,-1,0,0)$	$(0,0,-1,-2)$	$(0,0,2,-1)$
$(1,0,-2,0)$	$(0,1,0,-2)$	$(2,0,1,0)$	$(0,2,0,1)$
$(-1,0,2,0)$	$(0,-1,0,2)$	$(-2,0,-1,0)$	$(0,-2,0,-1)$
$(1,0,0,-2)$	$(0,1,2,0)$	$(0,-2,1,0)$	$(2,0,0,1)$
$(-1,0,0,2)$	$(0,-1,-2,0)$	$(0,2,-1,0)$	$(-2,0,0,-1)$

Bab selanjutnya akan menjelaskan tentang pemetaan yang dilakukan pada penelitian ini beserta dengan konstruksi fungsi *hash* dari graf ekspander LPS.

BAB 3

FUNGSI *HASH* DARI GRAF EKSPANDER LPS

Pada bab ini akan dibahas tentang pemetaan dari grup *quaternion* ke grup matriks berukuran 2×2 dengan operasi perkalian matriks, konstruksi fungsi *hash* dari graf ekspander LPS, dan teorema Tillich-Zemor mengenai serangan pada fungsi *hash* dari graf ekspander LPS yang menghasilkan tumbukan.

3.1. Pemetaan dari Grup *Quaternion* $H(\mathbf{Z}_p)$ ke $\mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$

Berikut ini adalah penjelasan dari Davidoff dkk. (2003) tentang pembentukan grup $\mathrm{PGL}_2(F)$.

Misalkan F suatu lapangan. $\mathrm{GL}_2(F)$ adalah grup matriks non singular berukuran 2×2 dengan setiap entrinya merupakan anggota dari F dengan operasi perkalian matriks. $\mathrm{PGL}_2(F)$ adalah grup kuosien dari $\mathrm{GL}_2(F)$ yang didefinisikan sebagai berikut

$$\mathrm{PGL}_2(F) = \mathrm{GL}_2(F) / \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} : \lambda \in F - \{0\} \right\}.$$

Proposisi berikut ini menjelaskan tentang order dari $\mathrm{GL}_2(F)$ dan $\mathrm{PGL}_2(F)$ jika F adalah lapangan hingga dengan order p.

Proposisi 3.1. (Davidoff, 2003) Jika F adalah suatu lapangan hingga dengan order p, maka

1. $|\mathrm{GL}_2(F)| = p(p-1)(p^2-1)$
2. $|\mathrm{PGL}_2(F)| = p(p^2-1)$

Bukti.

1. Ambil matriks $M \in \mathrm{GL}_2(F)$, artinya determinan $M \neq 0$, maka tidak ada kolom dari M yang merupakan vektor nol. Sehingga ada $p^2 - 1$ buah kolom pertama dari M yang bisa dipilih. Selanjutnya akan dipilih kolom kedua yang bebas linear dari kolom pertama. Pilihan untuk kolom kedua ini ada sebanyak $p^2 - p$. Maka banyaknya matriks M yang bisa dipilih

adalah $(p^2-1)(p^2-p) = p(p-1)(p^2-1)$.

Jadi $|\mathrm{GL}_2(F)| = p(p-1)(p^2-1)$.

2. Karena $\mathrm{PGL}_2(F)$ merupakan grup yang beranggotakan koset-koset kiri berbeda dari $H = \left\{\begin{bmatrix}\lambda & 0\\ 0 & \lambda\end{bmatrix} : \lambda \in F - \{0\}\right\}$ di $\mathrm{GL}_2(F)$ dan $H < \mathrm{GL}_2(F)$ maka berdasarkan Teorema 2.1 maka $|\mathrm{GL}_2(F)| = |\mathrm{PGL}_2(F)||H|$.

Karena $|F| = p$ maka $|H| = p-1$, dan $|\mathrm{GL}_2(F)| = p(p-1)(p^2-1)$ maka $|\mathrm{PGL}_2(F)| = \frac{p(p-1)(p^2-1)}{p-1} = p(p^2-1)$

Jadi $|\mathrm{PGL}_2(F)| = p(p^2-1)$. ■

Berikut ini akan didefinisikan suatu pemetaan dari suatu grup *quaternion* ke grup $\mathrm{PGL}_2(F)$ dengan $F = \mathbf{Z}_p \times \mathbf{Z}_p = \{a_0 + a_1\mathbf{i} : \mathbf{i}^2 \equiv -1 (\mathrm{mod}\ p), a_0, a_1 \in \mathbf{Z}_p\}$ dengan operasi penjumlahan $(a_0 + a_1\mathbf{i}) + (b_0 + b_1\mathbf{i}) = (a_0 + a_1) + (b_0 + b_1)\mathbf{i}$ dan operasi perkalian $(a_0 + a_1\mathbf{i})(b_0 + b_1\mathbf{i}) = (a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0)\mathbf{i}$.

Misalkan p suatu bilangan prima ganjil, $H(\mathbf{Z}_p)$ adalah grup *quaternion* dengan setiap anggotanya merupakan integral *quaternion* dengan norma tak nol dan operasi perkalian yang telah didefinisikan di Bab 2.2, dan $\mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$ adalah grup matriks non singular berorder 2 yang berbentuk $\begin{bmatrix} a+b\mathbf{i} & c+d\mathbf{i} \\ -c+d\mathbf{i} & a-b\mathbf{i}\end{bmatrix}$, dengan $\mathbf{i}^2 = -1 \pmod p$ dengan operasi perkalian matriks. Pemetaan f dari $H(\mathbf{Z}_p)$ ke $\mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$ didefinisikan sebagai berikut

$$f\big((a_0, a_1, a_2, a_3)\big) = \begin{bmatrix} a_0 + a_1\mathbf{i} & a_2 + a_3\mathbf{i} \\ -a_2 + a_3\mathbf{i} & a_0 - a_1\mathbf{i}\end{bmatrix}. \tag{3.1}$$

Dengan pemetaan ini maka *quaternion unit* mempunyai padanan matriks *unit*, yaitu $E = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, -E = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}, E_i = \begin{bmatrix}\mathbf{i} & 0\\ 0 & -\mathbf{i}\end{bmatrix}, -E_i = \begin{bmatrix}-\mathbf{i} & 0\\ 0 & \mathbf{i}\end{bmatrix}$, $E_j = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, -E_j = \begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}, E_k = \begin{bmatrix}0 & \mathbf{i}\\ \mathbf{i} & 0\end{bmatrix}, -E_k = \begin{bmatrix}0 & -\mathbf{i}\\ -\mathbf{i} & 0\end{bmatrix}$. Dua matriks A dan B dikatakan terhubung jika $A = \varepsilon B$, dengan ε adalah matriks *unit*. Lebih lanjut, karena determinan dari matriks *unit* adalah 1, maka determinan dari matriks A sama dengan determinan matriks B.

Contoh berikut menggambarkan matriks-matriks yang saling terhubung.

Contoh 3.1: Misalkan $A = \begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix}$, maka

$$EA = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix}$$

$$-EA = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} -1-2\mathbf{i} & 0 \\ 0 & -1+2\mathbf{i} \end{bmatrix}$$

$$E_iA = \begin{bmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} -2+\mathbf{i} & 0 \\ 0 & -2-\mathbf{i} \end{bmatrix}$$

$$-E_iA = \begin{bmatrix} -\mathbf{i} & 0 \\ 0 & \mathbf{i} \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} 2-\mathbf{i} & 0 \\ 0 & 2+\mathbf{i} \end{bmatrix}$$

$$E_jA = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} 0 & 1-2\mathbf{i} \\ -1-2\mathbf{i} & 0 \end{bmatrix}$$

$$-E_jA = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} 0 & -1+2\mathbf{i} \\ 1+2\mathbf{i} & 0 \end{bmatrix}$$

$$E_kA = \begin{bmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} 0 & 2+\mathbf{i} \\ -2+\mathbf{i} & 0 \end{bmatrix}$$

$$-E_kA = \begin{bmatrix} 0 & -\mathbf{i} \\ -\mathbf{i} & 0 \end{bmatrix}\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix} = \begin{bmatrix} 0 & -2-\mathbf{i} \\ 2-\mathbf{i} & 0 \end{bmatrix}$$

Jadi $\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix}, \begin{bmatrix} -1-2\mathbf{i} & 0 \\ 0 & -1+2\mathbf{i} \end{bmatrix}, \begin{bmatrix} -2+\mathbf{i} & 0 \\ 0 & -2-\mathbf{i} \end{bmatrix}, \begin{bmatrix} 2-\mathbf{i} & 0 \\ 0 & 2+\mathbf{i} \end{bmatrix},$
$\begin{bmatrix} 0 & 1-2\mathbf{i} \\ -1-2\mathbf{i} & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1+2\mathbf{i} \\ 1+2\mathbf{i} & 0 \end{bmatrix}, \begin{bmatrix} 0 & 2+\mathbf{i} \\ -2+\mathbf{i} & 0 \end{bmatrix}, \begin{bmatrix} 0 & -2-\mathbf{i} \\ 2-\mathbf{i} & 0 \end{bmatrix}$
adalah 8 matriks yang saling terhubung.

Lemma 3.1. Pemetaan f pada Persamaan (3.1) merupakan pemetaan bijektif.

Bukti.

(injektif) Ambil $q, r \in H(\mathbf{Z}_p)$ dan $f(q) = f(r)$, akan ditunjukkan bahwa $q = r$.

Misalkan $q = (a_0, a_1, a_2, a_3)$ dan $r = (b_0, b_1, b_2, b_3)$.

Maka $f(q) = \begin{bmatrix} a_0 + a_1\mathbf{i} & a_2 + a_3\mathbf{i} \\ -a_2 + a_3\mathbf{i} & a_0 - a_1\mathbf{i} \end{bmatrix}$ dan $f(r) = \begin{bmatrix} b_0 + b_1\mathbf{i} & b_2 + b_3\mathbf{i} \\ -b_2 + b_3\mathbf{i} & b_0 - b_1\mathbf{i} \end{bmatrix}$,

karena $f(q) = f(r)$ maka $a_0 + a_1\mathbf{i} = b_0 + b_1\mathbf{i}$ dan $a_2 + a_3\mathbf{i} = b_2 + b_3\mathbf{i}$,

sehingga diperoleh $a_0 = b_0, a_1 = b_1, a_2 = b_2$, dan $a_3 = b_3$. Dengan perkataan lain $q = r$. Artinya pemetaan f bersifat injektif.

(surjektif) Ambil $M \in \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$, akan ditunjukkan terdapat $q \in H(\mathbf{Z}_p)$ sedemikian sehingga $f(q) = M$.

Misalkan $M = \begin{bmatrix} a + b\mathbf{i} & c + d\mathbf{i} \\ -c + d\mathbf{i} & a - b\mathbf{i} \end{bmatrix}$.

$|M| = (a + b\mathbf{i})(a - bi) - (c + di)(-c + di) = a^2 + b^2 + c^2 + d^2 \neq 0$, dan

$a, b, c, d \in \mathbf{Z}_p$. Pilih $q = (a, b, c, d)$ maka $N(q) = a^2 + b^2 + c^2 + d^2 = |M|$, artinya $N(q) \neq 0$, sehingga $q \in H(\mathbf{Z}_p)$. Berdasarkan definisi pemetaan f, maka

$$f(q) = \begin{bmatrix} a + b\mathbf{i} & c + d\mathbf{i} \\ -c + d\mathbf{i} & a - b\mathbf{i} \end{bmatrix} = M.$$

Jadi untuk setiap $M \in \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$ maka terdapat $q \in H(\mathbf{Z}_p)$ sedemikian sehingga $f(q) = M$. Dengan perkataan lain pemetaan f bersifat surjektif. Dengan demikian dapat disimpulkan bahwa pemetaan f bersifat bijektif. ■

Berdasarkan Lemma 3.1 maka Teorema 2.3 dapat dimodifikasi menjadi pernyataan berikut ini.

Teorema 3.1. Misalkan $M \in \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p), |M| = 1 \pmod 2$, $|M| = \prod_{i=1}^{m} p_i$, dengan p_i adalah faktor prima dari $|M|$ maka $M = \prod_{i=1}^{m} A_i$, dengan $|A_i| = p_i$, untuk $i = 1, 2, \ldots, m$.

Dengan memodifikasi Teorema 3.1 di atas dengan melakukan proses perkalian matriks $A_1 A_2 \ldots A_{m-1}$ maka akan diperoleh akibat berikut.

Akibat 3.1. Misalkan $M \in \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$, $|M| = 1 \pmod 2$, $|M| = \prod_{i=1}^{m} p_i$, dengan p_i adalah faktor prima dari $|M|$ dan $m \neq 1$ maka $M = BA$, dengan $|A| = p_m$ dan $|B| = \prod_{i=1}^{m-1} p_i$.

Bukti. Ambil $M \in \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$, $|M| = 1 \ (mod\ 2)$, $|M| = \prod_{i=1}^{m} p_i$,. Maka berdasarkan Teorema 3.1, maka M dapat dinyatakan sebagai $M = \prod_{i=1}^{m} A_i$, dengan $|A_i| = p_i$, untuk $i = 1, 2, \ldots, m$. Karena perkalian matriks berlaku hukum asosiatif maka pernyataan di atas dapat dinyatakan dalam $M = (\prod_{i=1}^{m-1} A_i) A_m$. Misalkan $B = \prod_{i=1}^{m-1} A_i$ dan $A = A_m$, maka $|B| = \prod_{i=1}^{m-1} p_i$ dan $|A| = |A_m| = p_m$. Jadi $M = BA$. ■

Subbab berikutnya akan membahas tentang konstruksi fungsi *hash* dari graf ekspander LPS.

3.2. Konstruksi Fungsi *Hash* dari graf ekspander LPS.

Pembahasan pada subbab ini akan dibagi menjadi dua bagian. Bagian pertama akan menjelaskan tentang konstruksi graf ekspander LPS dan bagian kedua menjelaskan tentang konstruksi fungsi *hash* dari graf ekspander LPS.

3.2.1. Konstruksi Graf Ekspander LPS

Graf ekspander LPS adalah graf Cayley yang dibangun dari grup $\mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$, dengan p bilangan prima ganjil dan $p \equiv 1(\mathrm{mod}\ 4)$ dengan $S_p \subseteq \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$, dengan S_p didefinisikan sebagai berikut.

$$S_p = \left\{ M = \begin{bmatrix} a+b\mathbf{i} & c+d\mathbf{i} \\ -c+d\mathbf{i} & a-b\mathbf{i} \end{bmatrix} : |M| = p, a > 0 \right\}$$

dengan $a \equiv 1 \pmod 2$ dan $b \equiv c \equiv d \equiv 0 (\mathrm{mod}\ 2)$.

Jika $M = \begin{bmatrix} a+b\mathbf{i} & c+d\mathbf{i} \\ -c+d\mathbf{i} & a-b\mathbf{i} \end{bmatrix} \in S_p$, maka $\bar{M} = \begin{bmatrix} a-b\mathbf{i} & -c-d\mathbf{i} \\ c-d\mathbf{i} & a+b\mathbf{i} \end{bmatrix}$ disebut sebagai konjugat dari M dan $|\bar{M}| = |M|$, sehingga $\bar{M} \in S_p$. Konjugat dari M juga merupakan invers dari M, hal ini dapat ditunjukkan pada pernyataan berikut ini.

$$M\bar{M} = \begin{bmatrix} a+b\mathbf{i} & c+d\mathbf{i} \\ -c+d\mathbf{i} & a-b\mathbf{i} \end{bmatrix} \begin{bmatrix} a-b\mathbf{i} & -c-d\mathbf{i} \\ c-d\mathbf{i} & a+b\mathbf{i} \end{bmatrix}$$

$$= \begin{bmatrix} a^2+b^2+c^2+d^2 & 0 \\ 0 & a^2+b^2+c^2+d^2 \end{bmatrix}$$

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

$$\equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ karena } \begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^{-1} \in \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & \lambda \end{bmatrix} : \lambda \in F - \{0\} \right\}.$$

Sehingga S_p merupakan himpunan simetris.

Untuk menentukan order dari S_p dilakukan dengan langkah-langkah berikut ini.

1. Mencari banyaknya $M \in \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$ yang determinannya sama dengan p.

   $$|M| = \left| \begin{bmatrix} a+b\mathbf{i} & c+d\mathbf{i} \\ -c+d\mathbf{i} & a-b\mathbf{i} \end{bmatrix} \right| = (a+bi)(a-bi) - (c+di)(-c+di)$$
   $$= a^2+b^2+c^2+d^2,$$

   artinya untuk mencari banyaknya M yang determinannya p sama dengan mencari banyaknya solusi dari Persamaan (2.1), dan p bilangan prima,

maka faktor dari p adalah 1 dan p, sehingga diperoleh sebanyak $8(p+1)$ matriks yang berdeterminan p.

2. Mereduksi solusi pada langkah pertama dengan mempertahankan satu matriks dari matriks-matriks yang saling terhubung. Oleh karena terdapat 8 buah matriks *unit* berbeda, maka terdapat 8 buah matriks yang saling terhubung, artinya kedelapan matriks tersebut dapat direduksi menjadi 1 buah matriks. Sehingga banyaknya matriks yang tersisa dari hasil reduksi ini adalah $p+1$.

Jadi order dari S_p adalah $p+1$.

Tabel 3.1. Himpunan matriks-matriks yang berdeterminan **5**.

$\begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2+\mathbf{i} & 0 \\ 0 & -2-\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 0 & 1-2\mathbf{i} \\ -1-2\mathbf{i} & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 2+\mathbf{i} \\ -2+\mathbf{i} & 0 \end{bmatrix}$
$\begin{bmatrix} -1-2\mathbf{i} & 0 \\ 0 & -1+2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2-\mathbf{i} & 0 \\ 0 & 2+\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 0 & -1+2\mathbf{i} \\ 1+2\mathbf{i} & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & -2-\mathbf{i} \\ 2-\mathbf{i} & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}$	$\begin{bmatrix} \mathbf{i} & 2\mathbf{i} \\ 2\mathbf{i} & -\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2 & 1 \\ -1 & -2 \end{bmatrix}$	$\begin{bmatrix} -2\mathbf{i} & \mathbf{i} \\ \mathbf{i} & 2\mathbf{i} \end{bmatrix}$
$\begin{bmatrix} -1 & -2 \\ 2 & -1 \end{bmatrix}$	$\begin{bmatrix} -\mathbf{i} & -2\mathbf{i} \\ -2\mathbf{i} & \mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2 & -1 \\ 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 2\mathbf{i} & -\mathbf{i} \\ -\mathbf{i} & -2\mathbf{i} \end{bmatrix}$
$\begin{bmatrix} 1 & 2\mathbf{i} \\ 2\mathbf{i} & 1 \end{bmatrix}$	$\begin{bmatrix} \mathbf{i} & -2 \\ 2 & -\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2\mathbf{i} & 1 \\ -1 & -2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2 & \mathbf{i} \\ \mathbf{i} & -2 \end{bmatrix}$
$\begin{bmatrix} -1 & -2\mathbf{i} \\ -2\mathbf{i} & -1 \end{bmatrix}$	$\begin{bmatrix} -\mathbf{i} & 2 \\ -2 & \mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2\mathbf{i} & -1 \\ 1 & 2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2 & -\mathbf{i} \\ -\mathbf{i} & 2 \end{bmatrix}$
$\begin{bmatrix} 1-2\mathbf{i} & 0 \\ 0 & 1+2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2+\mathbf{i} & 0 \\ 0 & 2-\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 0 & 1+2\mathbf{i} \\ -1+2\mathbf{i} & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & -2+\mathbf{i} \\ 2+\mathbf{i} & 0 \end{bmatrix}$
$\begin{bmatrix} -1+2\mathbf{i} & 0 \\ 0 & -1-2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2-\mathbf{i} & 0 \\ 0 & -2+\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 0 & -1-2\mathbf{i} \\ 1-2\mathbf{i} & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 2-\mathbf{i} \\ -2-\mathbf{i} & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}$	$\begin{bmatrix} \mathbf{i} & -2\mathbf{i} \\ -2\mathbf{i} & -\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2 & 1 \\ -1 & 2 \end{bmatrix}$	$\begin{bmatrix} 2\mathbf{i} & \mathbf{i} \\ \mathbf{i} & -2\mathbf{i} \end{bmatrix}$
$\begin{bmatrix} -1 & 2 \\ -2 & -1 \end{bmatrix}$	$\begin{bmatrix} -\mathbf{i} & 2\mathbf{i} \\ 2\mathbf{i} & \mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2 & -1 \\ 1 & -2 \end{bmatrix}$	$\begin{bmatrix} -2\mathbf{i} & -\mathbf{i} \\ -\mathbf{i} & 2\mathbf{i} \end{bmatrix}$
$\begin{bmatrix} 1 & -2 \\ -2 & 1 \end{bmatrix}$	$\begin{bmatrix} \mathbf{i} & 2 \\ -2 & -\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2\mathbf{i} & 1 \\ -1 & 2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2 & \mathbf{i} \\ \mathbf{i} & 2 \end{bmatrix}$
$\begin{bmatrix} -1 & 2\mathbf{i} \\ 2\mathbf{i} & -1 \end{bmatrix}$	$\begin{bmatrix} -\mathbf{i} & -2 \\ 2 & \mathbf{i} \end{bmatrix}$	$\begin{bmatrix} 2\mathbf{i} & -1 \\ 1 & -2\mathbf{i} \end{bmatrix}$	$\begin{bmatrix} -2 & -\mathbf{i} \\ -\mathbf{i} & -2 \end{bmatrix}$

Contoh berikut ini menunjukkan langkah-langkah untuk membentuk himpunan pembangkit S_p dengan $p = 5$.

1. Mencari semua matriks dari $\mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$ yang nilai determinannya 5. Berdasarkan pada Lemma 3.1, maka *quaternion-quaternion* pada Contoh 2.14 dapat dipetakan menjadi matriks-matriks pada Tabel 3.1.
2. Selanjutnya akan dilakukan reduksi terhadap matriks-matriks di atas. Berdasarkan Contoh 3.1 maka dapat dilihat bahwa 2 baris pertama pada Tabel 3.1 merupakan matriks-matriks yang saling terhubung. Hal sama juga terjadi pada matriks-matriks pada baris ke-3 dengan ke-4, baris ke-5 dengan ke-6, baris ke-7 dengan ke-8, baris ke-9 dengan ke-10, dan baris ke-11 dengan baris ke-12. Dengan perkataan lain matriks-matriks pada pasangan baris tersebut dapat direduksi menjadi 1 matriks yang terhubung dengan matriks-matriks tersebut sehingga akan diperoleh 6 buah matriks. Dari setiap pasangan baris dipilih matriks yang memenuhi sifat-sifat himpunan S_p, yaitu

   $M_1 = \begin{bmatrix} 1+2\mathbf{i} & 0 \\ 0 & 1-2\mathbf{i} \end{bmatrix}, M_2 = \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, M_3 = \begin{bmatrix} 1 & 2\mathbf{i} \\ 2\mathbf{i} & 1 \end{bmatrix}$
   $, M_4 = \begin{bmatrix} 1-2\mathbf{i} & 0 \\ 0 & 1+2\mathbf{i} \end{bmatrix}, M_5 = \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}$, dan $M_6 = \begin{bmatrix} 1 & -2 \\ -2 & 1 \end{bmatrix}$.

   Jadi $S_p = \{M_1, M_2, M_3, M_4, M_5, M_6\}$.

Dari himpunan pembangkit S_p yang diperoleh pada penjelasan contoh di atas, konjugat dari M_1, M_2 dan M_3 berturut-turut adalah M_4, M_5 dan M_6. Oleh karena itu M_4, M_5 dan M_6 secara berturut-turut dapat ditulis sebagai $\overline{M_1}, \overline{M_2}$ dan $\overline{M_3}$. Sehingga himpunan pembangkit S_p pada contoh di atas dapat ditulis ulang menjadi $S_p = \{M_1, M_2, M_3, \overline{M_1}, \overline{M_2}, \overline{M_3}\}$.

Subbab berikutnya akan menjelaskan tentang konstruksi fungsi *hash* dari graf ekspander LPS yang dibangkitkan oleh himpunan pembangkit S_p.

3.2.2. Konstruksi Fungsi *Hash* dari graf ekspander LPS

Dalam penelitian ini fungsi *hash* dari graf ekspander LPS yang dibangkitkan oleh himpunan pembangkit S_p dinotasikan sebagai $\mathcal{H}$, berikut ini adalah langkah-langkah untuk membangun fungsi $\mathcal{H}$.

1. Pilih suatu fungsi $\pi: \{0, 1, 2, \dots, p-1\} \times S_p \to S_p$ sedemikian sehingga untuk setiap $A \in S_p$ maka himpunan $\pi(\{0, 1, 2, \dots, p-1\} \times \{A\})$ adalah $S_p - \{A^{-1}\}$.
2. Misalkan suatu pesan $\boldsymbol{x}$ dengan panjang $(k+1)$, $\boldsymbol{x} = x_0 x_1 \dots x_k$, $x_i \in \{0, 1, 2, \dots, p-1\}$ untuk $i = 0, 1, 2, \dots, k$. Definisikan suatu barisan $(A_i)_{0 \le i \le k}$ secara rekursif sebagai $A_i = \pi\big((x_i, A_{i-1})\big)$ dengan A_{-1} adalah nilai awal yang merupakan suatu anggota dari S_p.
3. Maka nilai dari fungsi *hash* $\mathcal{H}$ untuk pesan $\boldsymbol{x}$ didefinisikan sebagai $\mathcal{H}(\boldsymbol{x}) = A_{-1} A_0 A_1 \dots A_k$.

Berikut ini contoh untuk menghitung nilai fungsi *hash* $\mathcal{H}$ untuk suatu pesan $\boldsymbol{x} = 0114$ pada contoh graf ekspander dikonstruksi pada Subbab 3.2.1.

1. Definisikan fungsi π sebagai berikut.

π	M_1	M_2	M_3	$\overline{M_1}$	$\overline{M_2}$	$\overline{M_3}$
0	M_1	M_2	M_3	$\overline{M_1}$	$\overline{M_2}$	$\overline{M_3}$
1	M_2	M_3	$\overline{M_1}$	$\overline{M_2}$	$\overline{M_3}$	M_1
2	M_3	$\overline{M_1}$	$\overline{M_2}$	$\overline{M_3}$	M_1	M_2
3	$\overline{M_2}$	$\overline{M_3}$	M_1	M_2	M_3	$\overline{M_1}$
4	$\overline{M_3}$	M_1	M_2	M_3	$\overline{M_1}$	$\overline{M_2}$

2. Misalkan $A_{-1} = M_2$ dan pesan $\boldsymbol{x} = 11034$. Maka

$$A_0 = \pi\big((x_0, A_{-1})\big) = \pi\big((1, M_2)\big) = M_3$$
$$A_1 = \pi\big((x_1, A_0)\big) = \pi\big((1, M_3)\big) = \overline{M_1}$$
$$A_2 = \pi\big((x_2, A_1)\big) = \pi\big((0, \overline{M_1})\big) = \overline{M_1}$$
$$A_3 = \pi\big((x_3, A_2)\big) = \pi\big((3, \overline{M_1})\big) = M_2$$
$$A_4 = \pi\big((x_4, A_3)\big) = \pi\big((4, M_2)\big) = M_1$$

3. Jadi nilai *hash* untuk pesan $\boldsymbol{x} = 11034$ adalah

$$\mathcal{H}(\boldsymbol{x}) = A_{-1}A_0 \dots A_4 = M_2M_3\overline{M_1}\,\overline{M_1}M_2M_1$$

$$\mathcal{H}(\boldsymbol{x}) = \begin{bmatrix} 81+62\mathbf{i} & -48-54\mathbf{i} \\ 48-54\mathbf{i} & 81-62\mathbf{i} \end{bmatrix} \equiv \begin{bmatrix} 1+2\mathbf{i} & -3-4\mathbf{i} \\ 3-4\mathbf{i} & 1-2\mathbf{i} \end{bmatrix}.$$

Subbab berikutnya akan menjelaskan tentang tumbukan pada fungsi *hash* dari graf ekspander LPS.

3.3. Tumbukan pada Fungsi *Hash* dari graf ekspander LPS

Pada subbab ini akan dijelaskan bagaimana tumbukan pada fungsi *hash* dari graf ekspander LPS dapat dilakukan. Serangan yang menghasilkan tumbukan ini dipublikasikan oleh Tillich dan Zemor pada tahun 2008.

Untuk melakukan serangan terhadap konstruksi fungsi *hash* dari graf ekspander LPS, didefinisikan suatu himpunan Ω yang relevan terhadap himpunan pembangkit S_p. Jika $M \in \Omega$, maka M memenuhi syarat-syarat berikut:

1. $M \in \mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p), |M| = p^w$, untuk suatu $w \in \mathbf{N}$
2. $a > 0$ dan $a \equiv 1 \pmod 2$
3. $b \equiv c \equiv d \equiv 0 \pmod 2$.

Teorema 3.2. (Tillich-Zemor, 2008) Setiap matriks $M \in \Omega$ dapat dinyatakan sebagai faktorisasi unik

$$M = \pm p^r M_1 M_2 \cdots M_e \tag{3.2}$$

dengan $\log_p |M| = e + 2r$, $M_i \in S_p$ untuk $i = 1,2, \dots, e$, dan $M_i M_{i+1} \neq pE$ untuk $i \in \{1,2, \dots, e-1\}$.

Bukti.

(Eksistensi) Ambil $M \in \Omega$, artinya $|M| = p^w$, jika $w = 1$, maka M merupakan anggota dari S_p. Dengan menggunakan Akibat 3.1, maka M dapat dinyatakan sebagai perkalian dari matriks A_1B_1 dengan $|A_1| = p^{w-1}$ dan $|B_1| = p$ yaitu

$$M = A_1B_1 \tag{3.3}$$

Karena $|B_1| = p$ maka dapat diperoleh suatu $M_1' \in S_p$ yang terhubung dengan B_1 sehingga Persamaan (3.3) dapat dinyatakan sebagai

$$M = A_1\varepsilon_1 M_1', \text{ dengan } \varepsilon_1 \text{ matriks } unit \text{ dan } M_1' \in S_p \quad (3.4)$$

Selanjutnya $A_1\varepsilon_1$ akan dihitung dan hasilnya dilambangkan sebagai A_1', dan karena $|\varepsilon_1| = 1$, maka $|A_1'| = |A_1|$. Sehingga Persamaan (3.4) dapat ditulis sebagai

$$M = A_1'M_1', |A_1'| = p^{w-1}, M_1' \in S_p \quad (3.5)$$

Lakukan hal sama untuk matriks A_1' hingga Persamaan (3.5) menjadi

$$M = A_2'M_2'M_1', |A_2'| = p^{w-2}, M_2' \in S_p \quad (3.6)$$

Dengan melakukan hal sama berulang sebanyak $(w-3)$ kali, maka Persamaan (3.6) dapat ditulis menjadi

$$M = \varepsilon M_w'M_{w-1}' \dots M_2'M_1', |M_i'| = p, M_i' \in S_p, i = 1, 2, \dots, w \quad (3.7)$$

Kemudian dengan mereduksi bentuk-bentuk $M_i'M_{i-1}'$ yang bernilai pE maka akan diperoleh

$$M = p^r \varepsilon M_1 M_2 \dots M_e \quad (3.8)$$

dengan r menandakan banyaknya pasangan $M_i'M_{i-1}' = pE$ yang direduksi dan M_j merupakan M_i' yang tersisa dari reduksi yang dilakukan, $j \in \{1, 2, \dots, e\}$ sehingga $w = 2r + e$ atau dengan perkataan lain $|M| = p^w = p^{2r+e} \Leftrightarrow \log_p|M| = 2r + e$. Jadi pada Persamaan (3.8) tidak mengandung $M_iM_{i+1} = pE, i \in \{1, 2, \dots, e-1\}$.

(Ketunggalan) Untuk menentukan ketunggalan dari faktorisasi dari Persamaan (3.2) maka akan diperiksa banyaknya matriks berbeda pada ruas kiri dan banyaknya faktorisasi berbeda yang dibangun pada ruas kanan.

-. Ruas kiri : Untuk menentukan banyaknya matriks dari $\mathrm{PGL}_2(\mathbf{Z}_p \times \mathbf{Z}_p)$ yang berdeterminan p^w akan digunakan Teorema *Jacobi's four-square*. Jadi banyaknya matriks berbeda pada ruas kiri adalah $8(1 + p + p^2 + \dots + p^w)$.

-. Ruas kanan : Karena faktorisasi pada ruas kanan tidak mengandung $M_iM_{i+1} = pE, i \in \{1, 2, \dots, e-1\}$ dan $|S_p| = p + 1$, jika $e \geq 1$ maka banyaknya faktorisasi dengan yang bisa dibangun tanpa melibatkan matriks *unit* adalah $(p+1)p^{e-1}$ dan jika $e = 0$ maka semua matriks akan tereduksi menjadi E yang artinya hanya terdapat 1 faktorisasi. Karena $w = 2r + e$ maka $e = w - 2r$ dan terdapat 8 buah matriks *unit* yang berbeda maka banyak faktorisasi pada ruas kanan menjadi $8(p+1)p^{e-1}$ faktorisasi untuk $0 < e \leq \frac{w}{2}$ dan 8 faktorisasi untuk $e = 0$.

- Jika w suatu bilangan genap maka e bernilai genap yaitu $0,2,4,\dots,w$.

  $e = 0$ maka banyak faktorisasi adalah 8.

  $e = 2$ maka banyak faktorisasi adalah $8(p+1)p^{2-1} = 8(p^2+p)$

  $e = 4$ maka banyak faktorisasi adalah $8(p+1)p^{4-1} = 8(p^4+p^3)$

  $\vdots$

  $e = w$ maka banyak faktorisasi adalah $8(p+1)p^{w-1} = 8(p^w+p^{w-1})$.

  Sehingga seluruh faktorisasi yang bisa dibangun adalah

  $8(p^w+p^{w-1}) + \cdots 8(p^4+p^3) + 8(p^2+p) + 8 = 8(p^w+p^{w-1}+\cdots+ p^4+p^3+p^2+p+1)$.

- Jika w suatu bilangan ganjil maka e bernilai ganjil yaitu $1,3,5,\dots,w$.

  $e = 1$ maka banyak faktorisasi adalah $8(p+1)p^{1-1} = 8(p+1)$

  $e = 3$ maka banyak faktorisasi adalah $8(p+1)p^{3-1} = 8(p^3+p^2)$

  $e = 5$ maka banyak faktorisasi adalah $8(p+1)p^{5-1} = 8(p^5+p^3)$

  $\vdots$

  $e = w$ maka banyak faktorisasi adalah $8(p+1)p^{w-1} = 8(p^w+p^{w-1})$.

  Sehingga seluruh faktorisasi yang bisa dibangun adalah

  $8(p^w+p^{w-1}) + \cdots + 8(p^3+p^2) + 8(p+1) = 8(p^w+p^{w-1}+\cdots+ p^3+p^2+p+1)$.

Jadi banyaknya faktorisasi yang mungkin pada ruas kanan adalah $8(1+p+p^2+p^3+\cdots+p^w)$.

Karena banyaknya matriks M pada ruas kiri sama dengan banyaknya faktorisasi yang dapat dibangun pada ruas kanan, bersama dengan eksistensi dari faktorisasi dari matriks M maka dapat disimpulkan bahwa faktorisasi dari matriks M bersifat tunggal. ■

Pada bab selanjutnya akan dibahas tentang pengaruh transformasi himpunan pembangkit S_p menjadi $S_p{}^2$ terhadap serangan yang dilakukan oleh Teorema Tillich-Zemor dan beberapa sifat dari himpunan pembangkit $S_p{}^2$.

BAB 4

PENGARUH TRANSFORMASI HIMPUNAN PEMBANGKIT S_p MENJADI ${S_p}^2$ PADA FUNGSI *HASH* DARI GRAF EKSPANDER LPS

Pada bab ini akan membahas tentang transformasi himpunan pembangkit, sifat-sifat dari hasil transformasi dan pengaruhnya terhadap serangan yang dilakukan oleh Teorema Tillich-Zemor

Transformasi yang dilakukan adalah mengkuadratkan setiap anggota dari himpunan pembangkit S_p, yang dinotasikan sebagai ${S_p}^2 = \{M^2 : M \in S_p\}$.

Misalkan $\alpha \in S_p$ artinya α dapat dituliskan sebagai

$$\alpha = \begin{bmatrix} a_0 + a_1\mathbf{i} & a_2 + a_3\mathbf{i} \\ -a_2 + a_3\mathbf{i} & a_0 - a_1\mathbf{i} \end{bmatrix} \tag{4.1}$$

dengan $a_0, a_1, a_2, a_3 \in \mathbf{Z}_p$ dan memenuhi

$$a_0 \equiv 1 \pmod 2 \tag{4.2}$$

$$a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod 2 \tag{4.3}$$

$$|\alpha| = p \tag{4.4}$$

sehingga dengan mengkuadratkan α maka akan diperoleh

$$\alpha^2 = \begin{bmatrix} a_0 + a_1\mathbf{i} & a_2 + a_3\mathbf{i} \\ -a_2 + a_3\mathbf{i} & a_0 - a_1\mathbf{i} \end{bmatrix} \begin{bmatrix} a_0 + a_1\mathbf{i} & a_2 + a_3\mathbf{i} \\ -a_2 + a_3\mathbf{i} & a_0 - a_1\mathbf{i} \end{bmatrix}$$

$$\alpha^2 = \begin{bmatrix} ({a_0}^2 - {a_1}^2 - {a_2}^2 - {a_3}^2) + 2a_0a_1\mathbf{i} & 2a_0a_2 + 2a_0a_3\mathbf{i} \\ -2a_0a_2 + 2a_0a_3\mathbf{i} & ({a_0}^2 - {a_1}^2 - {a_2}^2 - {a_3}^2) - 2a_0a_1\mathbf{i} \end{bmatrix}$$

Jika $\beta = \begin{bmatrix} b_0 + b_1\mathbf{i} & b_2 + b_3\mathbf{i} \\ -b_2 + b_3\mathbf{i} & b_0 - b_1\mathbf{i} \end{bmatrix} \in {S_p}^2$ dengan $\beta = \alpha^2$ maka

$$b_0 = {a_0}^2 - {a_1}^2 - {a_2}^2 - {a_3}^2 \tag{4.5}$$

$$b_1 = 2a_0a_1 \tag{4.6}$$

$$b_2 = 2a_0a_2 \tag{4.7}$$

$$b_3 = 2a_0a_3 \tag{4.8}$$

dan $b_0, b_1, b_2, b_3 \in \mathbf{Z}_p$.

Berikut ini adalah sifat-sifat numerik dari anggota ${S_p}^2$ yang dapat diperoleh dari penjelasan di atas.

Sifat 4.1. Bilangan b_0 pada Persamaan (4.5) memenuhi $b_0 \equiv 1 \pmod 2$.

Bukti

Berdasarkan Persamaan (4.2) maka diperoleh ${a_0}^2 \equiv 1 \pmod 2$.

Berdasarkan Persamaan (4.3) maka diperoleh ${a_1}^2 \equiv {a_2}^2 \equiv {a_3}^2 \equiv 0 \pmod 2$.

Karena ${a_0}^2 \equiv 1 \pmod 2$ dan ${a_1}^2 \equiv {a_2}^2 \equiv {a_3}^2 \equiv 0 \pmod 2$ maka

$${a_0}^2 - {a_1}^2 - {a_2}^2 - {a_3}^2 \equiv 1 \pmod 2.$$

Karena menurut Persamaan (4.5), $b_0 = {a_0}^2 - {a_1}^2 - {a_2}^2 - {a_3}^2$ sehingga

$$b_0 \equiv 1 \pmod 2.$$ ■

Sifat 4.2. Bilangan b_1, b_2, dan b_3 berturut-turut pada Persamaan (4.6), Persamaan (4.7), dan Persamaan (4.8) memenuhi $b_1 \equiv b_2 \equiv b_3 \equiv 0 \pmod 2$.

Bukti

Berdasarkan Persamaan (4.6), $b_1 = 2a_0a_1$, maka $b_1 \equiv 0 \pmod 2$.

Berdasarkan Persamaan (4.7), $b_2 = 2a_0a_2$, maka $b_2 \equiv 0 \pmod 2$.

Berdasarkan Persamaan (4.8), $b_3 = 2a_0a_3$, maka $b_3 \equiv 0 \pmod 2$.

Jadi $b_1 \equiv b_2 \equiv b_3 \equiv 0 \pmod 2$. ■

Sifat 4.3. Jika $\beta \in {S_p}^2$ maka $|\beta| = p^2$.

Bukti

Misalkan $\beta = \begin{bmatrix} b_0 + b_1\mathbf{i} & b_2 + b_3\mathbf{i} \\ -b_2 + b_3\mathbf{i} & b_0 - b_1\mathbf{i} \end{bmatrix} \in {S_p}^2$, maka

$$\begin{aligned}
|\beta| &= (b_0 + b_1\mathbf{i})(b_0 - b_1\mathbf{i}) - (b_2 + b_3\mathbf{i})(-b_2 + b_3\mathbf{i}) \\
&= {b_0}^2 + {b_1}^2 + {b_2}^2 + {b_3}^2 \\
&= ({a_0}^2 - {a_1}^2 - {a_2}^2 - {a_3}^2)^2 + (2a_0a_1)^2 + (2a_0a_2)^2 + (2a_0a_3)^2 \\
&= ({a_0}^2 - ({a_1}^2 + {a_2}^2 + {a_3}^2))^2 + 4{a_0}^2({a_1}^2 + {a_2}^2 + {a_3}^2) \\
&= ({a_0}^2)^2 - 2{a_0}^2({a_1}^2 + {a_2}^2 + {a_3}^2) + ({a_1}^2 + {a_2}^2 + {a_3}^2)^2 \\
&\qquad +4{a_0}^2({a_1}^2 + {a_2}^2 + {a_3}^2) \\
&= ({a_0}^2)^2 + 2{a_0}^2({a_1}^2 + {a_2}^2 + {a_3}^2) + ({a_1}^2 + {a_2}^2 + {a_3}^2)^2 \\
&= ({a_0}^2 + {a_1}^2 + {a_2}^2 + {a_3}^2)^2
\end{aligned}$$

Karena ${a_0}^2 + {a_1}^2 + {a_2}^2 + {a_3}^2 = p$ maka $|\beta| = p^2$. ■

Sifat 4.4. Himpunan pembangkit ${S_p}^2$ merupakan himpunan simetris.

Bukti

Telah ditunjukkan pada Bab 3.2 bahwa S_p merupakan himpunan simetris, artinya jika $\alpha \in S_p$ maka $\alpha^{-1} \in S_p$. Misalkan $\beta \in {S_p}^2$, maka terdapat $\alpha \in S_p$ sedemikian sehingga $\beta = \alpha^2$. Akibatnya terdapat $\beta' \in {S_p}^2$ sedemikian sehingga $\beta' = (\alpha^{-1})^2$. Klaim bahwa β' adalah invers dari β.

$$\beta\beta' = \alpha^2(\alpha^{-1})^2 = \alpha(\alpha\alpha^{-1})\alpha^{-1} = \alpha E\alpha^{-1} = \alpha\alpha^{-1} = E$$

Jadi untuk setiap $\beta \in {S_p}^2$ maka $\beta^{-1} \in {S_p}^2$. Dengan perkataan lain himpunan pembangkit ${S_p}^2$ merupakan himpunan simetris. ■

Sifat 4.5. Order dari himpunan pembangkit ${S_p}^2$ adalah $p + 1$. Dengan perkataan lain $|{S_p}^2| = p + 1$.

Bukti

Jelas bahwa $|{S_p}^2| \leq p + 1$, karena anggota-anggota ${S_p}^2$ diperoleh dengan mengkuadratkan anggota-anggota S_p dan $|S_p| = p + 1$.

Andaikan $|{S_p}^2| < p + 1$ artinya terdapat $\alpha_1, \alpha_2 \in S_p$ dan $\alpha_1 \neq \alpha_2$ sedemikian sehingga $\beta = {\alpha_1}^2 = {\alpha_2}^2$. Berdasarkan Sifat 4.4 maka $|\beta| = p^2$, artinya $\beta \in \Omega$. Sehingga berdasarkan pada Teorema Tillich-Zemor maka terdapat faktorisasi unik untuk β dari matriks-matriks di himpunan S_p. Jadi $\alpha_1 = \alpha_2$ (terjadi kontradiksi dengan pengandaian di atas), sehingga seharusnya $|{S_p}^2|$ tidak kurang dari $p + 1$. Dengan perkataan lain $|{S_p}^2| = p + 1$. ■

Berdasarkan penjelasan di atas, dapat disimpulkan bahwa sebagian besar sifat-sifat numerik dari anggota himpunan pembangkit ${S_p}^2$ sama dengan sifat-sifat numerik dari anggota himpunan pembangkit S_p. Tabel 4.1 menggambarkan tentang perbandingan sifat-sifat numerik dari himpunan pembangkit S_p dengan himpunan pembangkit ${S_p}^2$.

Tabel 4.1. Perbandingan sifat-sifat numerik dari anggota himpunan pembangkit S_p dan $S_p{}^2$.

Himpunan pembangkit S_p	Himpunan pembangkit $S_p{}^2$
$\alpha = \begin{bmatrix} a_0 + a_1\mathbf{i} & a_2 + a_3\mathbf{i} \\ -a_2 + a_3\mathbf{i} & a_0 - a_1\mathbf{i} \end{bmatrix}$	$\beta = \begin{bmatrix} b_0 + b_1\mathbf{i} & b_2 + b_3\mathbf{i} \\ -b_2 + b_3\mathbf{i} & b_0 - b_1\mathbf{i} \end{bmatrix}$
$a_0 \equiv 1 \pmod 2$	$b_0 \equiv 1 \pmod 2$
$a_1 \equiv a_2 \equiv a_3 \equiv 0 \pmod 2$	$b_1 \equiv b_2 \equiv b_3 \equiv 0 \pmod 2$
$\lvert\alpha\rvert = p$	$\lvert\beta\rvert = p^2$
$\lvert S_p\rvert = p + 1$	$\lvert S_p{}^2\rvert = p + 1$
S_p merupakan himpunan simetris	$S_p{}^2$ merupakan himpunan simetris

Untuk mengimplementasikan Teorema Tillich-Zemor pada fungsi *hash* dari hasil transformasi himpunan pembangkit, maka diperlukan himpunan yang relevan dengan himpunan pembangkit $S_p{}^2$. Berdasarkan pembahasan sifat-sifat dari $S_p{}^2$ maka dapat dilihat bahwa perubahan yang terjadi adalah pada nilai determinan setiap anggota $S_p{}^2$ adalah p^2 sedangkan nilai determinan setiap anggota S_p adalah p. Oleh karena itu, himpunan yang relevan dengan $S_p{}^2$ pun mengalami perubahan yaitu pada nilai determinan anggota-anggotanya. Himpunan Ω^* yang relevan dengan $S_p{}^2$ didefinisikan sebagai berikut

$$\Omega^* = \left\{ M = \begin{bmatrix} a + b\mathbf{i} & c + d\mathbf{i} \\ -c + d\mathbf{i} & a - b\mathbf{i} \end{bmatrix} : |M| = p^{2w}, a > 0, w \in \mathbf{N} \right\}$$

dengan $a, b, c, d \in \mathbf{Z}_p, a \equiv 1 (\text{mod } 2),\ b \equiv c \equiv d \equiv 0 (\text{mod } 2)$.

Agar serangan yang didasarkan pada Teorema Tillich-Zemor menghasilkan tumbukan, maka setiap $M \in \Omega^*$ harus dapat dinyatakan dalam faktorisasi unik dari matriks-matriks di $S_p{}^2$. Ternyata hal ini tidak terpenuhi karena terdapat matriks pada Ω^*, sedemikian sehingga matriks tersebut tidak dapat dinyatakan dalam faktorisasi matriks-matriks di $S_p{}^2$. Berikut ini diberikan contoh bahwa Teorema Tillich-Zemor tidak dapat diimplementasikan pada fungsi *hash* yang dibangun dari himpunan pembangkit $S_p{}^2$.

Contoh 4.1: Misalkan $p = 5$ dan $w = 1$. Ambil $M = \begin{bmatrix} 1 + 4\mathbf{i} & 2 + 2\mathbf{i} \\ -2 + 2\mathbf{i} & 1 - 4\mathbf{i} \end{bmatrix}$. Maka

$|M| = 25 = 5^2$, artinya $M \in \Omega^*$ dan $M \in \Omega$. Dengan memandang $M \in \Omega$, maka terdapat faktorisasi unik untuk M, yaitu $M = \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}\begin{bmatrix} 1 & 2i \\ 2i & 1 \end{bmatrix}$, namun $\begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2i \\ 2i & 1 \end{bmatrix} \notin {S_p}^2$.

Jadi Teorema Tillich-Zemor tidak dapat diimplementasikan pada fungsi *hash* yang dibangkitkan oleh himpunan pembangkit ${S_p}^2$. Dengan demikian dapat disimpulkan bahwa fungsi *hash* dari graf ekspander LPS yang dibangkitkan oleh himpunan pembangkit ${S_p}^2$ aman dari serangan yang dilakukan oleh Tillich-Zemor.

Pada bab ini telah dijelaskan mengenai pengaruh transformasi himpunan pembangkit S_p menjadi himpunan pembangkit ${S_p}^2$ terhadap sifat-sifat numerik dari anggota-anggota himpunan pembangkit, dan menjelaskan bahwa fungsi *hash* dari graf ekspander yang dibangkitkan oleh himpunan pembangkit ${S_p}^2$ aman dari serangan yang dilakukan oleh Tillich-Zemor dengan memberikan suatu contoh penyangkal yang menunjukkan bahwa Teorema Tillich-Zemor tidak dapat diimplementasikan. Bab selanjutnya akan menjelaskan tentang kesimpulan dan saran dari penelitian ini.

BAB 5

KESIMPULAN DAN SARAN

Berdasarkan penjelasan pada bab-bab sebelumnya maka dapat diperoleh kesimpulan-kesimpulan berikut ini.

1. Sifat-sifat numerik dari anggota himpunan pembangkit $S_p{}^2$ sama dengan sifat-sifat numerik dari anggota himpunan pembangkit S_p, kecuali determinannya.
2. Transformasi himpunan pembangkit S_p menjadi $S_p{}^2$ mengakibatkan Teorema Tillich-Zemor tidak lagi berlaku walaupun sudah dilakukan transformasi untuk himpunan Ω menjadi himpunan Ω^* yang relevan terhadap himpunan pembangkit $S_p{}^2$. Akibat dari tidak berlakunya Teorema Tillich-Zemor adalah fungsi *hash* yang dibangun berdasarkan graf ekspander LPS dengan himpunan pembangkit $S_p{}^2$ menjadi lebih aman.

Dari hasil penelitian yang dilakukan, masih perlu dilakukan kajian lebih mendalam tentang kemungkinan adanya himpunan Ω^* lain yang relevan terhadap himpunan pembangkit $S_p{}^2$ sedemikian sehingga Teorema Tillich-Zemor dapat diimplementasikan pada fungsi *hash* dari graf ekspander LPS yang dibangkitkan oleh himpunan pembangkit $S_p{}^2$.

DAFTAR PUSTAKA

[1] Charles, D., Goren, E., dan Lauter, K. (2007). Cryptographic hash functions from expander graph. *Journal of Cryptology*, volume 22 halaman 93–113.

[2] Davidoff, G., Sarnak, P., dan Valette, A. (2003). *Elementary number theory, group theory, and Ramanujan graphs.* London Mathematical Society Student Texts, nomor 55. Cambridge University Press.

[3] Dickson, L. E. (1922). Arithmetics of quaternions, *Proc. London Math. Soc.* (2) 20, hal. 225-232.

[4] Hirschhorn, M. D. (1987). A simple proof of jacobi's four-square theorem, *Proc. of the American Mathematical Society*. volume 101, no. 3, hal. 436–438.

[5] Hungerford, T. W. (1993). *Algebra*. Springer, New York, United States of America.

[6] Linial, N. dan Wigderson, A. (2003). *Expander graphs and their applications*. Lecture notes, The Hebrew University, Israel.

[7] Lubotzky, A., Phillips, R., dan Sarnak, P. (1988). Ramanujan graphs. *Combinatorica 8*, volume 3, halaman 261–277.

[8] Petit, C. (2009). *On graph-based cryptographic hash functions.* PhD thesis, Universite Catholique de Louvain, Lauvain-la-Neuve.

[9] Pizer, A. K. (1990). Ramanujan Graphs and Hecke Operators, *Bulletin of The American Mathematical Society*, volume 23, no 1.

[10] Rosen, K. H. (2007). *Discrete mathematics and its applications*. Sixth Edition, McGraw-Hill, New York, United States of America.

[11] Tillich, J. P. dan Zemor, G. (2008). Collisions for the LPS expander graph hash function. Smart, N., Editor, *Advances in Cryptology (EUROCRYPT'08)*, The Theory and Applications of Cryptographic Techniques 27th Annual International Conference, halaman 254–269, Berlin/Heidelberg. Springer-Verlag.

[12] Windarta, S. (2010). *Fungsi hash kriptografis dari graf ekspander Lubotzky Phillips Sarnak*. Tesis, Universitas Indonesia, Depok.