UIN IMAM BONJOL PADANG

MAP Journal
Mathematics & Applications

Web : ejournal.uinib.ac.id/jurnal/index.php/MAp
Email : map_journal@uinib.ac.id

PEMILIHAN GRUP UNTUK KRIPTOSISTEM GTRU
CHOOSING GROUP FOR GTRU CRYPTOSYSTEM

Abdul Hadi[1§], Musraini[2], Sri Gemawati[3]

[1] Jurusan Matematika, FMIPA, Universitas Riau Jl. HR. Soebrantas KM. 12,5 Kampus Bina Widya, Simpang Baru, Pekanbaru, 28293, Indonesia [Email: abdulhadi@lecturer.unri.ac.id]

[2] Jurusan Matematika, FMIPA, Universitas Riau Jl. HR. Soebrantas KM. 12,5 Kampus Bina Widya, Simpang Baru, Pekanbaru, 28293, Indonesia [Email: musraini@lecturer.unri.ac.id]

[3] Jurusan Matematika, FMIPA, Universitas Riau Jl. HR. Soebrantas KM. 12,5 Kampus Bina Widya, Simpang Baru, Pekanbaru, 28293, Indonesia [Email: sri.gemawati@lecturer.unri.ac.id]

[§]*Corresponding Author*

Received Nov 10th 2021; Accepted Jun 30th 2022; Published Jun 30th 2022;

Abstrak

Kriptosistem kunci publik seperti NTRU yang didasarkan pada grup, dikenal dengan nama GTRU. Dalam pengkonstruksian GTRU, tidak semua grup dapat digunakan. Hal ini disebabkan proses dekripsi pada GTRU berhasil hanya pada grup dengan kondisi tertentu saja. Di [1], telah diberikan hanya dua contoh grup yang dapat digunakan untuk mengkonstruksi GTRU, yaitu suatu grup yang isomorfis dengan $\mathbb{Z}^n$ dan grup poly-$\mathbb{Z}$ $G_n = \mathbb{Z}^{n-3} \times \mathrm{H}$ dimana H adalah grup Heisenberg Diskrit yang dapat diaplikasikan pada internet of thing (IoT). Untuk memudahkan penggunaan GTRU, pada tulisan ini disediakan beberapa pilihan grup lain yang dapat digunakan untuk kriptosistem GTRU.

Kata Kunci: Grup, Subgrup Normal, Homomorfisma Grup, NTRU, GTRU

Abstract

Public key cryptosystems like NTRU that is based on group, known as GTRU. In GTRU construction, not all groups can be used. This is because the decryption process in GTRU is successful only to group with certain conditions. In [1]*, given only two examples of groups that can be used to construct a GTRU, i.e group* $\mathbb{Z}^{\{\phi_i : 1 \le i \le n\}}$ *and poly-*$\mathbb{Z}$ *group* $G_n = \mathbb{Z}^{n-3} \times \mathrm{H}$ *where* H *is a Discrete Heisenberg group that can be applied to the internet of things (IoT). This paper provides other groups that can be used to construct the GTRU cryptosystem.*

Keywords*: Group, Normal Subgroup, Homomorphism Group, NTRU, GTRU.*

1. Pendahuluan

Pesatnya perkembangan internet dan teknologi informasi saat ini mempengaruhi secara langsung kebutuhan informasi dalam kehidupan manusia. Berbagai kemudahan dan kenyamanan yang ditawarkan sekaligus dapat mengundang terjadinya tindakan kejahatan atau kriminalitas di dunia maya atau dunia siber yang motifnya tentulah ingin mengambil kesempatan dan keuntungan semata. Selain itu, minimnya keamanan data saat ini, membuat isi pesan mudah

terbaca oleh orang ketiga. Oleh karena itu, diperlukan sistem keamanan yang kuat dan sulit untuk ditembus para pihak yang tak bertanggung jawab. Salah satu solusi dalam menghadapi masalah ini adalah merancang kriptosistem kunci publik.

Ide kriptografi kunci publik pertama kali dikenalkan oleh Diffie Hellman [1] tahun 1976. Banyak kriptografi kunci publik yang telah dirancang seperti RSA [2], Kriptografi Kurva Eliptik (ECC) [3] dan McEliece [4] yang didasarkan pada masalah sulitnya memfaktorkan suatu bilangan yang besar dan sulitnya menemukan logaritma diskrit dari suatu grup berhingga. Dalam penerapannya, algoritmanya kurang efisien karena membutuhkan ruang yang besar dan kompleksitas perhitungan yang tinggi. Kriptosistem ini akan mudah dihancurkan oleh algoritma kuantum yang dikembangkan oleh Shor [5]. Namun, belakangan muncul tipe keamanan baru pada kriptosistem kriptografi yang didasarkan pada masalah sulit dalam struktur matematika yang disebut latis. Kriptosistem berdasarkan latis ini mempunyai keuntungan diantaranya enskripsi/deskripsi yang lebih cepat dan tahan terhadap komputer kuantum (maksudnya hingga saat ini tidak ada algoritma kuantum yang dengan cepat memecahkan masalah sulit latis). Salah satu kriptosistem yang berdasarkan latis adalah NTRU yang dikenalkan oleh Hoffstein, Pipher dan Silverman [6] pada tahun 1996 dengan menggunakan ring polinomial.

Dibandingkan dengan kriptosistem RSA dan kurva eliptik, NTRU memiliki keunggulan, yaitu komputasinya yang lebih efisien dibanding RSA dan Kurva eliptik. Karena itu, NTRU cocok untuk diterapkan pada perangkat portabel, smart card, ponsel, dll.

Banyak peneliti yang telah berusaha memperbaiki dan memodifikasi kriptosistem NTRU dengan tujuan untuk meningkatkan efisiensi dan keamanan dari NTRU, yang diantaranya dilakukan dengan penggantian struktur ring dengan struktur aljabar lain, memodifikasi parameter, algoritma pembentukan kunci, enkripsi dan dekripsinya serta menganalisis keamanannya [7]–[21].

Salah satu kriptosistem kunci publik seperti NTRU yang berdasarkan pada grup adalah GTRU [1] yang dikenalkan oleh Li Shuai tahun 2019. Kriptosistem ini merupakan perumuman dari NTRU dan diklaim lebih aman dari NTRU. Dalam pengkonstruksian GTRU, tidak semua grup dapat digunakan untuk mengkonstruksinya. Hal ini disebabkan proses dekripsi pada GTRU berhasil hanya pada grup yang memiliki setidaknya dua subgrup normal. Di [1], telah diberikan hanya dua contoh grup yang dapat digunakan untuk GTRU, yaitu grup $\mathbb{Z}^{\{\phi_i:1\le i\le n\}}$ yang isomorfis dengan $\mathbb{Z}^n$ dan grup poly-$\mathbb{Z}$ $G_n=\mathbb{Z}^{n-3}\times \mathrm{H}$ dimana H adalah grup Heisenberg Diskrit yang dapat diaplikasikan pada internet of thing (IoT). Untuk memudahkan dalam penggunaan GTRU, pada tulisan ini diberikan contoh grup-grup lain yang dapat digunakan untuk kriptosistem GTRU. Dalam penentuan grup untuk GTRU, diselidiki banyaknya subgrup normal nontrivial yang dimiliki oleh masing-masing grup.

2. Landasan Teori

Pada bagian ini, diberikan teori dasar dalam grup untuk digunakan dalam pembahasan nantinya.

Definisi 2.1. [22] *Misalkan G adalah himpunan tak kosong dan $*$ adalah operasi biner pada G. Himpunan G disebut grup terhadap operasi biner $*$, dinotasikan dengan $(G,*)$ jika memenuhi aksioma berikut:*

i. *Setiap $x, y \in G$ berlaku $x * y \in G$ (sifat tertutup)*
ii. $(x * y) * z = x * (y * z)$ *untuk setiap $x, y, z \in G$ (sifat asosiatif)*
iii. *Terdapat $e \in G$ sehingga $x * e = x = e * x$ untuk setiap $x \in G$ (eksistensi elemen netral)*
iv. *Untuk setiap $x \in G$ terdapat $y \in G$ sehingga $x * y = e = y * x$ (eksistensi elemen invers untuk setiap elemen di G). Dalam hal ini, y dikatakan invers dari x dan dinotasikan dengan $y = x^{-1}$.*

Selanjutnya, G disebut monoid jika memenuhi i, ii, iii. Jika G memenuhi aksioma i dan ii, maka G disebut semigrup. Jika operasi pada grup G bersifat komutatif, yaitu memenuhi kondisi $x * y = y * x$ untuk $x, y \in G$ maka G disebut grup abel atau grup komutatif. Untuk meringkas penulisan, selanjutnya $x * y$ cukup ditulis dengan xy.

Definisi 2.2. [22] *Himpunan bagian tak kosong H dari grup $(G,*)$ disebut subgrup dari G jika H merupakan grup terhadap operasi biner $*$ yang berlaku pada G.*

Teorema berikut menyatakan syarat perlu dan cukup suatu himpunan bagian dari grup merupakan suatu subgrup.

Proposisi 2.3. [22] *Himpunan bagian tak kosong H dari grup $(G,*)$ merupakan subgrup dari G jika dan hanya jika setiap $x, y \in H$ berlaku $x * y^{-1} \in H$.*

Definisi 2.4. [22] *Misalkan H adalah subgrup dari grup $(G,*)$. Himpunan $aH = \{ah \mid h \in H\}$ disebut koset kiri dari H pada G dan $Ha = \{ha \mid h \in H\}$ disebut koset kanan dari H pada G. Elemen a disebut representative (perwakilan) dari koset aH atau Ha.*

Secara umum, koset kiri dari suatu subgrup tidak selalu sama dengan koset kanannya. Jika koset kiri dari suatu subgrup selalu sama dengan koset kanannya, maka disebut subgrup normal. Berikut diberikan definisi formal dari subgrup normal.

Definisi 2.5. [22] *Misalkan H subgrup dari grup G. Subgrup H disebut subgrup normal dari G, dinotasikan dengan $H \triangleleft G$, jika untuk setiap $a \in G$ berlaku $aH = Ha$.*

Dari definisi subgrup normal, jelas bahwa setiap grup memiliki setidaknya dua subgrup normal yaitu subgrup trivial $\{e\}$ dan G itu sendiri. Jika grup G hanya memiliki subgrup normal $\{e\}$ dan G sendiri, maka grup G disebut grup sederhana (simple).

Proposisi 2.6. [22] *Misalkan H subgrup dari grup G. Subgrup H merupakan subgrup normal jika dan hanya jika untuk setiap $a \in G$ berlaku $aHa^{-1} \subseteq H$.*

Proposisi 2.7 [23] Center dari G, *yaitu*
$Z(G) = \{a \in G \mid ag = ga$ untuk setiap $g \in G\}$
merupakan subgrup normal dari G.

Proposisi 2.8 [23] Misal H adalah subgrup dari grup G. *Maka normalizer dari H di G, yaitu*
$$N(H) = \{x \in G \mid xHx^{-1} = H\}$$
merupakan subgrup normal dari G.

Proposisi 2.9. [23] *Jika G grup komutatif, maka subgrup dari G merupakan subgrup normal.*

Definisi 2.10. [23] *Misalkan H adalah subgrup normal dari grup G. Grup $G/H = \{aH \mid a \in G\}$ dengan operasi $\hat{*}$ yang didefinisikan sebagai $xH \hat{*} yH = xyH$ disebut grup faktor/kuosien dari G yang terbentuk oleh subgrup H.*

Definisi 2.11. [23] *Diberikan grup* $(G,*)$ *dan* $(G',*')$. *Pemetaan* $f:G\to G'$ *disebut homomorfisma grup jika berlaku* $f(x*y)=f(x)*'f(y)$ *untuk setiap* $x,y\in G$.

Proposisi 2.12. [23] Jika $f:G\to G'$ *homomorfisma grup, maka* $Ker(f)=\{x\in G: f(x)=e\}$ *merupakan subgrup normal dari G.*

Definisi 2.13. [23] *Homomorfisma* $f:G\to G'$ *yang injektif disebut monomorfisma grup, homomorfisma* $f:G\to G'$ *yang surjektif disebut epimorfisma, dan homomorfisma yang bijektif disebut isomorphism. Grup G dikatakan isomorfik dengan G', dinotasikan* $G\cong G'$ *jika terdapat suatu isomorfisma grup dari G ke G'. Selanjutnya, jika N subgroup normal dari G, maka homomorfisma* $\pi:G\to G/N$ *disebut homomorfisma natural. Homomorfisma dari G ke G disebut endomorfisma grup. Lebih lanjut, himpunan semua endomorfisma grup dari G ke G, dinotasikan dengan E(G). Himpunan E(G) merupakan monoid terhadap operasi komposisi fungsi.*

Definisi 2.14. [1] *Misal* N *subgrup normal dari G. Transversal ke* N *di* G *adalah himpunan* $T_N=\{t\in G\mid \bigcup tN=G\}$.

Proposisi 2.15. [23] Homomorfisma $f:G\to G'$ *adalah injektif jika dan hanya jika* $Ker(f)=\{e\}$.

Proposisi 2.16. [1] *Misal* G *adalah grup dan* N *adalah subgrup normal dari G,* $\pi_N:G\to G/N$ *homomorfisma natural, dan* T_N *adalah transversal ke* N *di G. Untuk setiap* $a\in G$, *dinotasikan elemen tunggal di* $aN\cap T_N$ *dengan* a_{T_N}, *maka fungsi* $\rho_{T_N}:G/N\to G$ *dengan* $\rho_{T_N}(aN)=a_{T_N}$ *terdefinisi dengan baik. Selanjutnya, berlaku* $\rho_{T_N}\circ\pi_N(t)=t$ *untuk setiap* $t\in T_N$.

Proposisi 2.17. [1] *Misal* G *adalah grup dan* N *adalah subgrup normal dari G,* $E(G)$ *endomorfisma monoid dari* G, $E(G/N)$ *endomorfisma monoid dari* G/N. *Dinotasikan* $E(G)_N=\{f\in E(G): f(N)\subseteq N\}$, *maka fungsi* $\bar{\pi}_N:E(G)_N\to E(G/N)$ *dengan* $\bar{\pi}_N(f)=\bar{f}$ *adalah homomorfisma monoid, dimana* $\bar{f}(xN)=f(x)N$. *Selanjutnya, misalkan* $\pi_N:G\to G/N$ *homomorfisma natural, maka berlaku* $\pi_N\circ f=\bar{\pi}_N(f)\circ\pi_N$ *untuk setiap* $f\in E(G)_N$.

Selanjutnya dibahas bagaimana kriptosistem GTRU bekerja menggunakan grup.

Diberikan grup G, subgroup normal N, transversal T_N dan homomorfisma grup $\pi_N,\rho_{T_N},\bar{\pi}_N$ yang telah dijelaskan di Proposisi 2.16 dan 2.17.

Parameter GTRU : Grup $(G,*)$, dua subgrup normal P dan Q dari G, transversal T_P,T_Q dan himpunan bagian $L_f,L_g\subseteq E(G)$.

Pembentukan Kunci: Pilih $f\in L_f, g\in L_g$ sedemikian hingga terdapat f_P, f_Q yang memenuhi

$\bar{\pi}_P(f_P\circ f)\circ\pi_P=\pi_P$ dan $\bar{\pi}_Q(f\circ f_Q)\circ\pi_Q=\pi_Q$.

Kemudian hitung kunci publik $h=\bar{\pi}_Q(f_Q\circ g)$ dan simpan kunci rahasia (f,g).

Enkripsi: Untuk mengenkripsi pesan $m\in L_m$, pilih secara acak $r\in L_r$, dan hitung

$$c=\pi_Q(m)h\circ\pi_Q(r).$$

Dekripsi: Untuk mendekripsi c, hitung pesan

$$m=\rho_{T_P}\circ\bar{\pi}_P(f_P)\circ\pi_P\circ\rho_{T_Q}\circ\bar{\pi}_Q(f)(c).$$

Dekripsi diatas tidak selalu berhasil dilakukan. Berikut ini diberikan syarat agar proses dekripsi pada GTRU berjalan dengan baik.

Proposisi 2.18. [1] Dekripsi GTRU dapat bekerja dengan benar jika parameter dari GTRU, yaitu G, P, Q,T_P dan T_Q memenuhi kondisi berikut.

D1. $L_f,L_g\subseteq E(G)_P\cap E(G)_Q$;

D2. $L_m \subseteq T_P$;
D3. $L_r \subseteq P$;
D4. $\{f(m)*g(r): f \in L_f, m \in L_m, g \in L_g, r \in L_r\} \subseteq T_Q$.

3. Hasil Dan Pembahasan

Pada [1], telah diberikan dua grup yang dapat digunakan pada GTRU, yaitu grup $\mathbb{Z}^{\{\phi_i:1\le i\le n\}}$ dan grup poly-$\mathbb{Z}$ $G_n = \mathbb{Z}^{n-3} \times \mathrm{H}$ dimana H adalah grup Hensenberg Diskrit. Pada bagian ini diberikan beberapa contoh grup selain dua grup tersebut sebagai alternatif dalam penggunaan GTRU.

Pada GTRU, parameter yang dipakai adalah grup $(G,*)$ dengan dua subgrup normal P dan Q, transversal T_P, T_Q dan himpunan bagian $L_f, L_g \subseteq E(G)$. Karena setiap grup G setidaknya memiliki dua subgrup normal yaitu subgrup normal trivial $\{e\}$ dan G itu sendiri, maka tentu setiap grup bisa digunakan pada GTRU. Namun, jika diambil subgrup normal trivial $\{e\}$ dan G itu sendiri, maka jelas untuk setiap homomorfisma grup $f: G \to G$, selalu memenuhi $f(e_G) = e_G$ dan $f(g) \in G$ untuk setiap $g \in G$. Karena itu, kita punya $f(\{e_G\}) \subseteq \{e_G\}$ dan $f(G) \subseteq G$, sehingga

$$E(G)_{\{e\}} = E(G)_G = E(G).$$

Jadi, pada Proposisi 2.18, untuk $P = \{e\}$ dan $Q = G$, diperoleh

D1. $L_f, L_g \subseteq E(G)_{\{e\}} \cap E(G)_G = E(G)$
D2. $L_m \subseteq T_{\{e\}} = G$
D3. $L_r \subseteq \{e\}$;
D4. $\{f(m)*g(r): f \in L_f, m \in L_m, g \in L_g, r \in L_r\} \subseteq T_G = \{e\}$.

Dari D1 dapat dilihat bahwa ukuran ruang kunci L_f untuk kunci f dan L_g untuk g adalah sebarang endomorfisma grup, Namun, pada kondisi D3 dan D4 haruslah $r = e$ dan $f(m)*g(r) = e$.

Karena $r = e$, dan f, g homomorfisma grup, berakibat

$$\begin{aligned} f(m)*g(r) &= e \\ f(m)*g(e) &= e \\ f(m)*e &= e \\ f(m) &= e \end{aligned}$$

yang berarti $m \in Ker(f) \subseteq G$. Ini jelas tidak efektif mengingat pemilihan r tidak acak lagi karena harus sama dengan e dan ruang pesan m adalah $L_m = Ker(f)$.

Jika diambil $P = G$ dan $Q = \{e\}$, maka

D1. $L_f, L_g \subseteq E(G)_G \cap E(G)_{\{e\}} = E(G)$
D2. $L_m \subseteq T_G = \{e\}$
D3. $L_r \subseteq G$;
D4. $\{f(m)*g(r): f \in L_f, m \in L_m, g \in L_g, r \in L_r\} \subseteq T_{\{e\}} = G$.

Ini berarti pesan yang dienkripsi hanyalah e.

Oleh karena itu, dengan memilih subgrup normal trivial akan membuat proses dekripsi tetap berjalan dengan baik namun tidak efektif untuk digunakan. Jadi, dalam pemilihan grup untuk GTRU, haruslah grup yang memiliki sedikitnya dua subgrup normal selain subgrup normal trivial. Dengan kata lain, grup yang digunakan untuk GTRU bukanlah grup sederhana (simple).

Sebagai contoh, grup $\mathbb{Z}_p$ dengan p prima dan grup alternating A_n untuk $n \ge 5$ (yaitu himpunan semua permutasi genap dari grup simetri S_n) adalah grup sederhana, sehingga tidak bisa digunakan untuk GTRU.

Berikut ini dibahas beberapa grup yang bisa

digunakan untuk GTRU dengan mencari subgrup normal nontrivialnya.

a) Grup bilangan bulat $(\mathbb{Z},+)$.

Himpunan $n\mathbb{Z}$ dengan $n \in \mathbb{Z}^{\geq 0}$ merupakan subgrup dari $(\mathbb{Z},+)$. Karena $(\mathbb{Z},+)$ grup komutatif, maka berdasarkan Proposisi 2.9, $n\mathbb{Z}$ merupakan subgrup normal dari $(\mathbb{Z},+)$. Jadi, semua subgrup normal $n\mathbb{Z}$ untuk $n \geq 2$ dapat digunakan sebagai parameter GTRU.

b) Grup bilangan bulat modulo $(\mathbb{Z}_n,+)$. Himpunan $k\mathbb{Z}_n$ dimana $k \in \mathbb{Z}$ merupakan subgrup dari $(\mathbb{Z}_n,+)$. Karena $(\mathbb{Z}_n,+)$ grup komutatif, maka berdasarkan Proposisi 2.9, $k\mathbb{Z}_n$ merupakan subgrup normal dari $(\mathbb{Z}_n,+)$. Untuk n komposit, $(\mathbb{Z}_n,+)$ bukan grup sederhana sehingga memiliki lebih dari dua subrup normal.

c) Grup matriks

$$GL_n(\mathbb{R}) = \{A \in M_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0\}$$

terhadap operasi perkalian matriks, himpunan

$$H = \{B \in M_{n\times n}(\mathbb{R}) \mid \det(B) = 1\}$$

merupakan subgrup normal dari $GL_n(\mathbb{R})$. Selain itu, normalizer dari H di $GL_n(\mathbb{R})$, yaitu

$$N(H) = \{X \in GL_n(\mathbb{R}) \mid XH = HX\}$$

juga merupakan subgrup normal dari $GL_n(\mathbb{R})$.

d. Grup permutasi S_n, yaitu grup himpunan semua permutasi dari $A = \{1,2,...,n\}$ dengan operasi komposisi fungsi.

Untuk $n = 3$, permutasi f pada $A = \{1,2,3\}$ adalah

$$f_0 = (1),\ f_1 = (1,2,3),\ f_2 = (1,3,2),$$

$$f_3 = (2,3),\ \ f_4 = (1,2),\ \ f_5 = (1,3).$$

Sehingga grup permutasi

$$S_3 = \{f_0, f_1, f_2, f_3, f_4, f_5\}$$

memiliki subgrup

$$\{f_0\}, \{f_0, f_1\}, \{f_0, f_2\}, \{f_0, f_5\}, \{f_0, f_3, f_4\}, S_3.$$

Namun, subgrup normal nontrivial dari S_3 hanyalah $\{f_0, f_3, f_4\} = \langle f_3 \rangle = A_3$. Karena itu, grup S_3 tidak bisa digunakan pada GTRU

Selain itu, subgrup normal nontrivial dari S_4 adalah A_4 dan

$$N = \{(1), (1,2)(3,4), (1,4)(3,2), (1,3)(2,4)\}.$$

Secara umum, A_n adalah subgrup normal dari S_n untuk $n = 2,...,70.$

e. Grup dihedral D_{2n}, yaitu himpunan rotasi dan refleksi dari *n*-gon

$$D_{2n} = \langle x, y : x^n = e, y^2 = e, y^{-1}xy = x^{-1} \rangle.$$

Untuk grup dihedral D_8 yang berarti grup himpunan rotasi dan refleksi dari 4-gon. Diperoleh

$D_8 = \{\delta_1, \delta_2, \delta_3, \delta_4, \mu_1, \mu_2, \rho_1, \rho_2\}$, dimana

$\delta_1 = (1), \delta_2 = (1,2,3,4), \delta_3 = (1,3)(2,4), \delta_4 = (1,4,3,2)$
$\mu_1 = (1,2)(3,4), \mu_2 = (1,4)(2,3), \rho_1 = (1,3), \rho_2 = (2,4)$

Grup D_8 ini jelas tidak komutatif karena $\rho_2\mu_2 \neq \mu_2\rho_2$. Adapun subgrup yang terdapat di D_8 adalah

$$\{\delta_1\}, \{\delta_1, \mu_1\}, \{\delta_1, \mu_2\}, \{\delta_1, \delta_3\}, \{\delta_1, \rho_1\}, \{\delta_1, \rho_2\},$$
$$\{\delta_1, \delta_3, \mu_1, \mu_2\}, \{\delta_1, \delta_2, \delta_3, \delta_4\}, \{\delta_1, \delta_3, \rho_1, \rho_2\}, D_8.$$

Namun, subgrup normal nontrivialnya adalah

$\{\delta_1,\delta_3\},\{\delta_1,\delta_3,\mu_1,\mu_2\},\{\delta_1,\delta_2,\delta_3,\delta_4\},\{\delta_1,\delta_3,\rho_1,\rho_2\}$.

f. Grup Quaternion

$Q_8=\{e,x,x^2,x^3,y,xy,x^2y,x^3y\}$.

yaitu grup yang dibangun oleh dua elemen x dan y yang memenuhi $o(x)=4,\ x^2=y^2$ dan $yx=x^3y$.

Selanjutnya diperoleh semua subgrup dari Q_8, yaitu $K_0=\{e\}$, $K_1=\{e,x^2\}$, $K_2=\{e,x,x^2,x^3\}$, $K_3=\{e,xy,x^2,x^3y\}$, $K_4=\{e,y,x^2,x^2y\}$ dan Q_8. Karena $[Q_8:K_2]=[Q_8:K_3]=[Q_8:K_4]=2$, maka K_2,K_3, dan K_4 adalah subgrup normal dari Q_8. Selain itu,

$yx^2y^{-1}=yxxy^{-1}=x^3yxy^{-1}=x^3x^3yy^{-1}=x^2\in K_1$.

Karena $Q_8=<x,y>$, maka K_1 adalah subgrup normal dari Q_8. Jadi, setiap subgrup dari Q_8 adalah subgrup normal.

4. Kesimpulan dan Saran

Grup yang dapat digunakan di GTRU harus memiliki sedikitnya dua subgrup normal nontrivial, seperti Grup bilangan bulat $(\mathbb{Z},+)$, Grup $(\mathbb{Z}_n,+)$ dengan *n* komposit, Grup matriks $GL_n(\mathbb{R})$, Grup permutasi S_4, Grup Dihedral D_8 dan Grup Quaternion Q_8. Namun, semua grup sederhana atau grup yang tidak memiliki subgrup normal nontrivial tidak dapat digunakan untuk GTRU seperti grup $\mathbb{Z}_p$ dengan *p* prima dan grup ganti tanda A_n, $n\geq 5$.

5. Ucapan Terima Kasih

Terimakasih kepada Fakultas matematika dan Ilmu Pengetahuan Alam Universitas Riau yang telah membantu mendanai penulisan artikel ini.

Daftar Pustaka

[1] L. Shuai, H. Xu, L. Miao, and X. Zhou, "A Group-based NTRU-like Public-key Cryptosystem for IoT," *IEEE Access*, vol. 7, pp. 75732–75740, 2019.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun ACM*, vol. 26, no. 1, pp. 96–99, 1983.

[3] N. Koblitz, "Elliptic curve cryptosystems," *Math Comput*, vol. 48, no. 177, pp. 203–209, 1987.

[4] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, vol. 4244, pp. 114–116, 1978.

[5] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, 1994, pp. 124–134.

[6] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *International algorithmic number theory symposium*, 1998, pp. 267–288.

[7] W. D. Banks and I. E. Shparlinski, "A variant of NTRU with non-invertible polynomials," in *International Conference on Cryptology in India*, 2002, pp. 62–70

[8] P. Gaborit, Julien Ohler, and Patrick Solé, *a polynomial analogue of NTRU*. Inria: Doctoral Dissertation, Inria, 2002.

[9] M. Coglianese and B.-M. Goi, "MaTRU: A new NTRU-based cryptosystem," in *International conference on cryptology in India*, 2005, pp. 232–243.

[10] R. Kouzmenko, "Generalizations of the NTRU cryptosystem," *Diploma Project, École Polytechnique Fédérale de Lausanne,(2005–2006)*, 2006.

[11] K. Jarvis and M. Nevins, "ETRU: NTRU over the Eisenstein integers," *Designs, Codes and Cryptography*, vol. 74, no. 1, pp. 219–242, 2015.

[12] N. Vats, "NNRU, a noncommutative analogue of NTRU," *arXiv preprint arXiv:0902.1891*, 2009.

[13] E. Malekian and A. Zakerolhosseini, "OTRU: A non-associative and high speed public key cryptosystem," in *2010 15th CSI international symposium on computer architecture and digital systems*, 2010, pp. 83–90.

[14] E. Malekian, A. Zakerolhosseini, and A. Mashatan, "QTRU: quaternionic version of the NTRU public-key cryptosystems," *The ISC International Journal of Information Security*, vol. 3, no. 1, pp. 29–42, 2011.

[15] A. K. Nanda, R. Nayak, and L. K. Awasthi, "NTRU with Gaussian integer matrix," *Int J Adv Res Comput Sci Software Eng*, vol. 5, pp. 359–365, 2015.

[16] A. H. Karbasi and R. E. Atani, "ILTRU: An NTRU-like public key cryptosystem over ideal lattices," *Cryptology ePrint Archive*, 2015.

[17] H. R. Yassein and N. M. G. Al-Saidi, "HXDTRU Cryptosystem Based on Hexadecnion Algebra," 2016.

[18] N. M. G. Alsaidi and H. R. Yassein, "BITRU: binary version of the NTRU public key cryptosystem via binary algebra," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 11, 2016.

[19] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, "NTRU prime: reducing attack surface at low cost," in *International Conference on Selected Areas in Cryptography*, 2017, pp. 235–260.

[20] H. R. Yassein and N. M. G. Al-Saidi, "BCTRU: A New Secure NTRU Crypt Public Key System Based on a Newly Multidimensional Algebra," in *proceeding of 6th international cryptology and information security conference*, 2018, pp. 1–11.

[21] W. Diffie and M. E. Hellman, "New Directions in Cryptography, 1976," *IEEE Transactions on Information Theory*, vol. 22, no. 6, 2011.

[22] D. S. M. J. N. Mordeson, M. K. Sen, and D. S. Malik, "Fundamentals Of Abstract Algebra," *The McCGraw-HILL Companies, Inc. New York st. Louis, san Francisco, printed in Singapore*, 1997.

[23] S. Wahyuni, I. E. Wijayanti, A. Munandar, and N. Hajriati, *Teori Representasi Grup Hingga*. Yogyakarta: Gadjah Mada University Press, 2018.