GRUP RSA MERUPAKAN GRUP *PSEUDO-FREE* DI BAWAH ASUMSI RSA KUAT

Khussal Zamlahani ۞, Dr. Agung Lukito, M. S. ۞,
۞ Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Surabaya
Jl. Ketintang Surabaya 60231
email : zamlahani@yahoo.com, zamlahani@gmail.com

ABSTRAK

Di bawah asumsi RSA kuat, dibuktikan bahwa grup perkalian modulo hasil kali dua prima selamat merupakan grup *pseudo-free*. Dengan kata lain, jika permasalahan RSA kuat sulit secara asimtotik berkenaan dengan distribusi ensembel $\mathcal{N}$ atas hasil kali dua bilangan prima selamat berbeda, maka keluarga grup komputasional $\mathbb{Z}_N^*$ ($N = PQ$, dengan P dan Q bilangan prima selamat berbeda, dengan operasi perkalian modulo dan prosedur sampling seragam atas QR_N) merupakan grup *pseudo-free* berkenaan dengan ensembel distribusi yang sama.

Keywords: asumsi RSA kuat, grup RSA, residu kuadratik, *pseudo-free*, prima selamat.

PENDAHULUAN

Kriptosistem RSA merupakan enkripsi kunci-publik (asimetris), yaitu menggunakan kunci yang berbeda dalam enkripsi dan dekripsi. Untuk mengenkripsi suatu pesan digunakan persamaan $c = m^e \bmod n$ dengan m adalah representasi bilangan bulat (dalam $\mathbb{Z}_n$) pesan/*plaintext* (teks, gambar, suara, dsb.), $n = pq$ adalah hasil kali dua bilangan prima (acak, berbeda, cukup besar, berukuran bit sama), e adalah kunci publik (bersama dengan n) yang merupakan bilangan bulat dengan $1 < e < \phi(n)$ (dengan $\phi(n) = (p-1)(q-1)$ menyatakan banyak bilangan bulat positif kurang dari n yang relatif prima dengan n), yang relatif prima dengan $\phi(n)$. Sedangkan untuk mengenkripsi digunakan persamaan $m = c^d \bmod n$ dengan c adalah *ciphertext*, dan d adalah kunci privat yang merupakan invers perkalian e modulo $\phi(n)$.

Telah diasumsikan oleh Rivest [6] bahwa tidak mungkin (mudah dengan peluang yang tak terabaikan) dengan menggunakan algoritma efisien apapun untuk mencari solusi $x \in \mathbb{Z}_n^*$ dan $e > 1$ dari persamaan $x^e \equiv a (\bmod n)$ dengan input $a \in \mathbb{Z}_n^*$ yang dipilih secara acak dan n adalah hasil kali dua bilangan prima besar yang dipilih secara acak. Singkatnya, sangat sulit bagi seseorang yang mengetahui *ciphertext* dan salah satu kunci publik n untuk mencari tahu *plaintext* dengan menggunakan suatu algoritma yang efisien dan kunci publik e yang ia pilih sendiri. Asumsi tersebut disebut dengan Asumsi RSA Kuat.

Grup *pseudo-free* memiliki syarat yang diperlukan agar permasalahan tersebut menjadi sulit. Secara informal, sebuah grup hingga G dikatakan *pseudo-free* jika tidak ada algoritma probabilistik berwaktu polinomial yang bisa secara efisien menghasilkan sebuah persamaan nontrivial E berikut solusinya di G dimana E tidak memiliki solusi di grup bebas.

Tulisan ini merupakan studi literatur dari sebuah paper yang berjudul *The RSA group is pseudo-free* karangan Daniele Micciancio. Dalam tulisan ini dibuktikan bahwa di bawah asumsi RSA kuat dengan ensembel distribusi $\mathcal{N}$ atas hasil kali prima selamat, keluarga grup komputasional $\mathbb{Z}_N^*$ (dengan operasi perkalian modulo, dan prosedur sampling seragam atas QR_N) merupakan grup *pseudo-free* berkenaan dengan ensembel distribusi yang sama.

Sistematika penulisan dimulai dengan pendahuluan pada bagian 1. Dasar teori pada bagian 2 yang mendasari pembahasan. Kemudian bagian 3 merupakan pembahasan/pembuktian dari teorema inti dan beberapa lemma yang mendukungnya. Bagian 4 berisi kesimpulan dari bagian 3.

DASAR TEORI

Grup Bebas & Persamaan Grup

Definisi 1

Misalkan $A = \{a_1, a_2, \ldots, a_l\}$. Untuk setiap a_i, misalkan a_i^{-1} invers a_i. Misalkan $A^{-1} = \{a_i^{-1} | a_i \in A\}$, dan misalkan $A^{\pm 1} = (A \cup A^{-1})$. Misalkan $F(A)$ himpunan kata dalam bentuk kanonik atas $A^{\pm 1}$, bersama dengan operasi $\cdot$ yaitu konkatenasi yang diikuti dengan reduksi hingga menghasilkan kata dalam bentuk kanonik, dapat dibuktikan bahwa $F(A)$ membentuk sebuah grup. Grup ini disebut **grup bebas** dan A disebut **pembangun** $F(A)$. Untuk selanjutnya diperbolehkan menulis $F(a_1, a_2, \ldots, a_l)$ jika $A = \{a_1, a_2, \ldots, a_l\}$.

Definisi 2
Misalkan X dan A berturut-turut himpunan hingga variabel dan konstanta yang saling lepas. Didefinisikan $X^{-1} = \{x^{-1}: x \in X\}$ dan $A^{-1} = \{a^{-1}: a \in A\}$. **Persamaan grup** atas variabel-variabel X dan konstanta-konstanta A adalah pasangan $E = (w_1, w_2)$, biasa ditulis $E: w_1 = w_2$, dengan $w_1 \in F(X)$ dan $w_2 \in F(A)$. Sebuah **solusi** persamaan $E: w_1 = w_2$ (atas grup bebas $F(A)$) merupakan sebuah fungsi $\sigma: X \to F(A)$, sedemikianhingga $\sigma(w_1) = w_2$ (dalam $F(A)$), dengan σ homomorfis yaitu $\sigma(x_1 x_2 \dots x_k) = \sigma(x_1)\sigma(x_2)\dots\sigma(x_k)$, σ dapat diperluas ke dalam kata-kata atas $F(X)$ dan $\sigma(x_i^{-1}) = \sigma(x_i)^{-1}$ untuk setiap $x_i \in X$. Persamaan $E: w_1 = w_2$ dikatakan **terpenuhi** (atas grup bebas) jika dan hanya jika E memiliki solusi. Jika tidak, maka E dikatakan **tak-terpenuhi**.

Definisi 3
Misalkan G grup (komputasional). **Persamaan grup** atas G (dinotasikan E_α) didefinisikan sebagai sebuah persamaan E atas variabel X dan konstanta A, dan sebuah fungsi $\alpha: A \to G$ dengan $\alpha(a_1 a_2 \dots a_l) = \alpha(a_1)\alpha(a_2)\dots\alpha(a_l)$, dan $\alpha(a_i^{-1}) = \alpha(a_i)^{-1}$ untuk setiap $a_i \in A$. **Solusi** persamaan $E_\alpha: w_1 = w_2$ merupakan fungsi $\xi: X \to G$ sedemikian hingga $\xi(w_1) = \alpha(w_2)$, dengan ξ homomorfis yaitu $\xi(x_1 x_2 \dots x_k) = \xi(x_1)\xi(x_2)\dots\xi(x_k)$, ξ dapat diperluas ke dalam kata-kata atas $F(X)$ dan $\xi(x_i^{-1}) = \xi(x_i)^{-1}$ untuk setiap $x_i \in X$.

Residu Kuadratik Modulo *N*

Definisi 4
Sebuah elemen $g \in \mathbb{Z}_N^*$ dikatakan **residu kuadratik** jika dan hanya jika $g = h^2 \bmod N$ untuk suatu $h \in \mathbb{Z}_N^*$. Himpunan residu kuadratik modulo N dinotasikan QR_N, dan merupakan subgrup $\mathbb{Z}_N^*$. Elemen $\mathbb{Z}_N^*$ yang bukan residu kuadratik disebut juga sebagai **nonresidu kuadratik**.

Definisi 5
Grup $\mathbb{Z}_N^*$ disebut **grup RSA** jika dan hanya jika $N = P \cdot Q$ dengan P dan Q merupakan bilangan prima berbeda.

Definisi 6
Bilangan prima P disebut **prima selamat** jika dan hanya jika $\frac{P-1}{2}$ juga merupakan bilangan prima.

Ensembel, Fungsi Terabaikan

Definisi 7
Misalkan I himpunan indeks terbilang. Sebuah **ensembel berindeks *I*** adalah barisan variabel acak berindeks I. Katakanlah, sebarang $\mathcal{X} = \{X_i\}_{i \in I}$, dengan tiap X_i adalah variabel acak, merupakan ensembel berindeks I.

Definisi 8
Sebuah fungsi $f: \mathbb{N} \to \mathbb{R}$ dikatakan **terabaikan** jika dan hanya jika menurun lebih cepat daripada sebarang polinomial invers. Dengan kata lain, untuk sebarang bilangan bulat $c > 0$ ada k_0 sedemikian hingga $|f(k)| \leq \frac{1}{k^c}$ untuk setiap $k > k_0$.

Asumsi RSA Kuat

Definisi 9
Algoritma berwaktu polinomial adalah algoritma yang fungsi waktu jalan kasus-terburuknya dalam bentuk $O(k^c)$ dengan k adalah ukuran input dan c adalah suatu konstanta. Sebarang algoritma yang waktu jalannya tidak bisa dibatasi disebut **algoritma berwaktu eksponensial**.

Definisi 10
Sebuah permasalahan komputasional (dengan parameter k) dikatakan **sulit secara asimtotik** jika dan hanya jika untuk setiap algoritma probabilistik berwaktu polinomial (dalam k), peluang algoritma tersebut menyelesaikan permasalahan tersebut merupakan fungsi yang terabaikan (dalam k).

Asumsi 1
Tidak mungkin bagi suatu algoritma probabilistik berwaktu polinomial, diberikan bilangan bulat n yang merupakan hasil kali dua bilangan prima yang cukup besar yang dipilih secara acak, dan sebuah elemen a dipilih secara acak dari $\mathbb{Z}_n^*$, untuk memperhitungkan $x \in \mathbb{Z}_n^*$ dan bilangan bulat $e > 1$ sedemikian hingga

$$x^e \equiv a \pmod n$$

dengan peluang yang tak terabaikan.

Grup Komputasional

Definisi 11
Misalkan $\mathcal{G} = \{G_N\}_{N \in \mathcal{N}}$ keluarga grup hingga yang diberi indeks $N \in \mathcal{N} \subseteq \{0,1\}^*$. **Keluarga grup komputasional** (terkait dengan $\mathcal{G}$) didefinisikan sebagai sebuah koleksi fungsi representasi $[\cdot]_N: G_N \to \{0,1\}^*$ sedemikian hingga operasi-operasi berikut dapat dilakukan dalam waktu polinomial (probabilistik, berukuran $\lg N$):

1) Menguji keanggotaan dalam grup: diberikan $N \in \mathcal{N}$ dan $x \in \{0,1\}^*$, tunjukkan bahwa $x = [y]_N$ merupakan representasi dari sebuah elemen grup $y \in G_N$.
2) Menghitung operasi grup: diberikan $N \in \mathcal{N}$, $[x]_N$ dan $[y]_N$ (untuk sebarang $x, y \in G_N$) hitung $[x * y]_N$.

3) Mencari invers elemen grup: diberikan $N \in \mathcal{N}$ dan $[x]_N$ (untuk suatu $x \in G_N$), cari $[x^{-1}]_N$.
4) Menghitung representasi elemen indentitas grup: diberikan $N \in \mathcal{N}$, $[e]_N$, dengan e elemen identitas grup G_N.
5) Sampling: dengan input $N \in \mathcal{N}$, menghasilkan output representasi $[x]$ dari sebuah elemen grup $x \in G_N$ yang dipilih secara acak.

Grup *Pseudo-free*

Definisi 12

Keluarga grup komputasional $\mathcal{G} = \{G_N\}_{N\in\mathcal{N}}$ dikatakan ***pseudo-free*** jika dan hanya jika untuk sebarang himpunan A berkardinalitas polinomial $|A| = p(k)$ (dengan k adalah ukuran bit N) dan algoritma probabilistik berwaktu polinomial (dalam k) $\mathcal{A}$, memenuhi syarat berikut ini: Misalkan $N \in \mathcal{N}_k$ indeks grup yang dipilih secara acak dan $\alpha: A \to G_N$ sebuah fungsi yang mendefinisikan $|A|$ elemen grup yang dipilih secara acak berdasarkan prosedur sampling pada grup komputasional. peluang $\mathcal{A}(N,\alpha) = (E,\xi)$ menghasilkan output sebuah persamaan E (atas variabel X dan konstanta A) yang tak terpenuhi bersama dengan solusi $\xi: X \to G_N$ milik E_α atas G_N, merupakan fungsi yang terabaikan dalam k.

PEMBAHASAN

Bagian ini berisi 5 lemma pendukung dan satu teorema utama disertai buktinya.

Lemma 1

Jika $N = PQ$ hasil kali dua bilangan prima selamat berbeda dan $\gamma \in \mathrm{QR}_N$ residu kuadratik, maka γ merupakan pembangun QR_N jika dan hanya jika $\gcd(\gamma - 1, N) = 1$.

Bukti:

Misalkan $P = 2p + 1$ dan $Q = 2q + 1$, dengan p dan q adalah bilangan prima berbeda. Dengan menggunakan *Chinese Remainder Theorem*, QR_N isomorfis dengan $\mathrm{QR}_P \times \mathrm{QR}_Q$ dengan isomorfisme

$$f(\gamma) = (\gamma_p, \gamma_q) = (\gamma \bmod P, \gamma \bmod Q).$$

Karena $|\mathrm{QR}_P| = \frac{P-1}{2} = p$ dan $|\mathrm{QR}_Q| = \frac{Q-1}{2} = q$, kita peroleh $|\mathrm{QR}_N| = pq$. Misalkan $o(\gamma_p)$ dan $o(\gamma_q)$ berturut-turut orde γ_p di QR_P dan orde γ_q di QR_Q. Pastilah $o(\gamma_p) \in \{1, p\}$ dan $o(\gamma_q) \in \{1, q\}$ dan $o(\gamma) = o(\gamma_p) \cdot o(\gamma_q) \in \{1, p, q, pq\}$. Perhatikan bahwa γ adalah pembangun QR_N jika dan hanya jika $o(\gamma) = |\mathrm{QR}_N| = pq$ atau secara ekuivalen $o(\gamma_p) = p$ dan $o(\gamma_q) = q$. Misalkan $g = \gcd(\gamma - 1, N)$. Karena $g | N$, maka $g \in \{1, P, Q, PQ\}$. Akan dibuktikan bahwa $o(\gamma) = pq$ jika dan hanya jika $g = 1$.

($\Rightarrow$)Pertama-tama andaikan $g \neq 1$; dengan kata lain, $g \in \{P, Q, PQ\}$. Maka $P|g$ atau $Q|g$. Tanpa mengurangi keterumuman, diperoleh $P|(\gamma - 1)$ sehingga $\gamma \equiv 1 (\mathrm{mod}\, P)$, karenanya $\gamma_p = 1$. Sehingga $o(\gamma_p) = 1$ dan $o(\gamma) \neq pq$.

($\Leftarrow$)Kemudian andaikan $o(\gamma) \neq pq$; dengan kata lain, $o(\gamma_p) = 1 \vee o(\gamma_q) = 1$. Asumsikan tanpa mengurangi keterumuman bahwa $o(\gamma_p) = 1$. Maka $\gamma \equiv \gamma_p \equiv 1 (\mathrm{mod}\, P)$. Sehingga $P|(\gamma - 1)$ dan karena $P|N$, maka $P|g$. Jadi $g \neq 1$. □

Lemma 2

Untuk sebarang grup siklik G dengan pembangun γ, jika $v \in \mathbb{Z}_B$ dipilih secara acak seragam, maka jarak statistik antara γ^v dan distribusi seragam atas G paling besar $\frac{|G|}{2B}$.

Bukti:

Perhatikan bahwa untuk sebarang $\gamma^i \in G$ dengan $i \in \mathbb{Z}_{|G|}$ berlaku $\gamma^v = \gamma^i$ jika dan hanya jika $v \equiv i (\mathrm{mod} |G|)$. Misalkan $V = \{v \in \mathbb{Z}_B : v \equiv i (\mathrm{mod} |G|)\}$ dan misalkan $|V| = n$. Diketahui

$$\mathbb{Z}_B = \{0, 1, \dots, v_1, \dots, v_2, \dots, v_n, \dots, B - 1\}$$

dengan $v_j \in V$ untuk setiap $1 \leq j \leq n$ dan $v_j < v_h \Leftrightarrow j < h$ dan pastilah $v_1 = i$. Karena

$$\left|\{v_j, v_j + 1, \dots, v_{j+1} - 1\}\right| = |G|$$

untuk setiap $1 \leq j < n$, maka

$$|\{v_1, v_1 + 1, \dots, v_n - 1\}| = (n-1)|G|.$$

Misalkan $|\{v_n, v_n + 1, \dots, B - 1\}| = t$, maka

$$B = i + (n-1)|G| + t$$

$$B - i = (n-1)|G| + t.$$

Jelaslah $t \leq |G|$ sehingga $\frac{t}{|G|} \leq 1$ dan $\left\lceil \frac{t}{|G|} \right\rceil = 1$. Sehingga diperoleh

$$1 = \left\lceil \frac{t}{|G|} \right\rceil$$

$$n - 1 + 1 = n - 1 + \left\lceil \frac{t}{|G|} \right\rceil$$

$$n = \frac{(n-1)|G|}{|G|} + \left\lceil \frac{t}{|G|} \right\rceil$$

$$n = \left\lceil \frac{(n-1)|G| + t}{|G|} \right\rceil$$

$$n = \left\lceil \frac{B-i}{|G|} \right\rceil.$$

Oleh karena itu, peluang $\gamma^v = \gamma^i$ adalah

$$\Pr\{\gamma^v = \gamma^i\} = \Pr\{v \equiv i (\mathrm{mod}|G|)\} = \frac{\left\lceil \frac{B-i}{|G|} \right\rceil}{B}$$

Karena $i + t < 2|G|$, maka $(i+t) - |G| < |G|$ dan tentu saja $|G| - (i+t) < |G|$ sehingga

$$\big||G| - (i+t)\big| < |G|$$

$$\big||G| - (i+t) + n|G| - n|G|\big| < |G|$$

$$\big|n|G| - i - t + |G| - n|G|\big| < |G|$$

$$|n|G| - (i + t - |G| + n|G|)| < |G|$$

$$|n|G| - (i + t + (n-1)|G|)| < |G|$$

$$|n|G| - B| < |G|$$

$$\frac{|n|G| - B|}{|G|} < 1$$

$$\frac{1}{B}\frac{|n|G| - B|}{|G|} < \frac{1}{B}$$

$$\left|\frac{n|G| - B}{B|G|}\right| < \frac{1}{B}$$

$$\left|\frac{n}{B} - \frac{1}{|G|}\right| < \frac{1}{B}$$

$$\left|\frac{1}{B}\left\lceil \frac{B-i}{|G|} \right\rceil - \frac{1}{|G|}\right| < \frac{1}{B}.$$

Oleh karena itu,

$$\left|\Pr\{\gamma^v = \gamma^i\} - \frac{1}{|G|}\right| = \left|\frac{1}{B}\left\lceil \frac{B-i}{|G|} \right\rceil - \frac{1}{|G|}\right| < \frac{1}{B}$$

Maka, jarak statistik antara γ^i dan distribusi seragam atas G

$$\frac{1}{2}\sum_{i=0}^{|G|-1}\left|\Pr\{\gamma^v = \gamma^i\} - \frac{1}{|G|}\right| < \frac{|G|}{2B}$$

seperti yang diinginkan. □

Lemma 3

Untuk sebarang keluarga grup komputasional $\mathcal{G}$, ada algoritma berwaktu polinomial dengan input persamaan E atas konstanta A dan variabel X, grup $G \in \mathcal{G}$, dan pengaitan (*assignment*) variabel $\xi: X \to G$, menghasilkan output persamaan satu variabel E' dan nilai $\xi' \in G$, sedemikian hingga

1) jika E tak terpenuhi atas grup bebas $F(A)$, maka E' juga tak terpenuhi atas $F(A)$; dan
2) untuk sebarang pengaitan $\alpha: A \to G$, jika ξ adalah solusi E_α, maka ξ' adalah solusi E'_α.

Bukti:

Misalkan inputnya persamaan $E: \prod_{x\in X} x^{e_x} = \prod_{a\in A} a^{d_a}$ dan fungsi pengaitan $\xi: X \to G$ dari variabel X ke grup G. Dengan menggunakan Algoritma Euclid yang Diperluas, hitung $e = \gcd(e_x : x \in X)$ dan bilangan bulat e'_x sedemikian hingga $\sum_{x\in X} e_x e'_x = e$. Dipilih persamaan output

$$E': x^e = \prod\nolimits_{a\in A} a^{d_a}$$

dengan solusi

$$\xi'(x) = \prod\nolimits_{x\in X} \xi(x)^{\frac{e_x}{e}}$$

Akan dibuktikan bahwa persamaan output ini memiliki sifat-sifat yang disyaratkan.

1) andaikan E' memiliki solusi di $F(A)$. Misalkan $\sigma' \in F(A)$ solusi E'; dengan kata lain, $(\sigma')^e = \prod_{a\in A} a^{d_a}$. Untuk setiap $x \in X$, definisikan $\sigma(x) = (\sigma')^{e'_x}$. Karena

$$\sigma\left(\prod_x x^{e_x}\right) = \prod_x \sigma(x)^{e_x} = \prod_x (\sigma')^{e'_x e_x}$$
$$= (\sigma')^{\sum_x (e_x e'_x)} = (\sigma')^e$$
$$= \prod\nolimits_{a\in A} a^{d_a}$$

Ini berarti bahwa σ solusi E di $F(A)$. Ini menunjukkan bahwa E terpenuhi atas grup bebas $F(A)$ pula, dan ini membuktikan sifat pertama.

2) ambil sebarang pengaitan $\alpha: A \to G$, dan misalkan $\xi: X \to G$ adalah solusi untuk E_α; dengan kata lain, $\prod_x \xi(x)^{e_x} = \prod_a a^{d_a}$ di G. Maka

$$\left(\xi'(x)\right)^e = \left(\prod_x \xi(x)^{\frac{e_x}{e}}\right)^e = \prod_x \xi(x)^{e_x}$$
$$= \prod\nolimits_a a^{d_a};$$

dengan kata lain, ξ' adalah solusi E'_α atas G. □

Sebelum pembahasan dilanjutkan ke lemma berikutnya, akan disajikan analisis berikut. Misalkan A himpunan berkardinalitas $|A| = p(k)$, untuk suatu $k \in \mathbb{N}$. Misalkan $v_a \in \{0, 1, \ldots, N|A|K - 1\}$ dengan $N = PQ = (2p+1)(2q+1)$ dengan P dan Q bilangan prima selamat dan $K \in \mathbb{Z}, K > 0$. Untuk setiap $a \in A$, misalkan $w_a = v_a \bmod pq$ dan $z_a = \frac{v_a - w_a}{pq}$.

Perhatikan bahwa jika diberikan w_a, maka distribusi z_a seragam atas himpunan

$$S_a = \left\{0,1,\dots,\left\lfloor\frac{N|A|K-1-w_a}{pq}\right\rfloor\right\}$$

berkardinalitas

$$|S_a| = \left\lfloor\frac{N|A|K-1-w_a}{pq}\right\rfloor + 1$$
$$= \left\lfloor\frac{N|A|K-1-w_a}{pq} + 1\right\rfloor$$
$$= \left\lfloor\frac{N|A|K-1-w_a+pq}{pq}\right\rfloor$$

karena $w_a \leq pq-1$, maka $pq-1-w_a \geq 0$. Karena

$$N = PQ = (2p+1)(2q+1)$$
$$= 4pq + 2(p+q) + 1 > 4pq,$$

maka

$$\frac{N}{pq} > 4.$$

Sehingga paling sedikit

$$|S_a| = \left\lfloor\frac{N|A|K-1-w_a+pq}{pq}\right\rfloor \geq \left\lfloor\frac{N|A|K}{pq}\right\rfloor$$
$$\geq 4|A|K \geq 4$$

Juga, jika diberikan w_a, maka nilai $\alpha(a) = \gamma^{v_a} = \gamma^{w_a}$ dapat ditentukan secara tunggal, dan z_a terdistribusi seragam atas himpunan S_a.

Lemma 4
Peluang bersyarat bahwa $d = \sum_a v_a d_a \neq 0$ paling sedikit $\frac{3}{4}$. (diberikan α, $e = 0$, dan $\{d_a : a \in A\}$ sedemikian hingga $e \nmid \gcd(d_a : a \in A)$)

Bukti:

Diketahui bahwa $v_a = w_a + pqz_a$, dengan tiap $z_a \in S_a$ dipilih secara acak seragam dari himpunan dengan kardinalitas $|S| \geq 4$. Karena $e \nmid \gcd(d_a : a \in A)$, maka ada $\dot{a} \in A$ sedemikian hingga $d_{\dot{a}} \neq 0$. Atur nilai v_a untuk setiap $a \neq \dot{a}$. Karena $d = 0$ untuk paling banyak satu nilai dari $z_{\dot{a}} \in S_{\dot{a}}$, dan $z_{\dot{a}}$ bebas dari pandangan $\mathcal{A}$, peluang bersyarat $d = 0$ paling besar $\frac{1}{|S_{\dot{a}}|} \leq \frac{1}{4}$. □

Lemma 5
Peluang bersyarat e tidak membagi $d = \sum_a v_a d_a$ paling sedikit $\frac{3}{8}$. (diberikan α, $\gcd(e, pq) = 1$, dan $\{d_a : a \in A\}$ sedemikian hingga $e \nmid \gcd(d_a : a \in A)$)

Bukti:

Karena $e \nmid \gcd(d_a : a \in A)$, maka e tidak membagi $d_{\dot{a}}$ untuk suatu $\dot{a} \in A$. Ingat bahwa $v_a = w_a + pqz_a$, dimana distribusi bersyarat dari z_a (w_a yang diberikan) seragam atas himpunan S_a. Selain itu, karena $\gcd(e, pq) = 1$, maka pq memiliki invers perkalian modulo e. Selesaikan persamaan $d \equiv 0 (\mathrm{mod}\, e)$ untuk $z_{\dot{a}}$, diperoleh

$$\sum_a v_a d_a \equiv 0 (\mathrm{mod}\, e)$$

$$v_{\dot{a}} d_{\dot{a}} + \sum_{a \neq \dot{a}} v_a d_a \equiv 0 (\mathrm{mod}\, e)$$

$$pqz_{\dot{a}} + w_{\dot{a}} \equiv -\sum_{a \neq \dot{a}} v_a d_a \,(\mathrm{mod}\, e)$$

$$z_{\dot{a}} \equiv -\frac{\sum_{a \neq \dot{a}}(v_a d_a) + w_{\dot{a}}}{pq} (\mathrm{mod}\, e)$$

Karena $z_{\dot{a}}$ dipilih secara acak seragam dalam interval $S_{\dot{a}}$, dengan menggunakan prinsip sangkar merpati, ini terjadi dengan peluang paling besar

$$\frac{\left\lceil\frac{|S_{\dot{a}}|}{e}\right\rceil}{|S_{\dot{a}}|} \leq \frac{|S_{\dot{a}}| + e - 1}{e \cdot |S_{\dot{a}}|} = \frac{1}{e} + \frac{1}{|S_{\dot{a}}|} - \frac{1}{e \cdot |S_{\dot{a}}|} \leq \frac{5}{8}.$$

Di sini telah digunakan fakta bahwa $|S_{\dot{a}}| \geq 4$ dan $e \geq 2$ merupakan bilangan bulat. Jadi, $e \nmid d$ dengan peluang paling sedikit $\frac{3}{8}$. □

Teorema 1
Jika permasalahan RSA kuat sulit secara asimtotik berkenaan dengan distribusi ensembel $\mathcal{N}$ atas hasil kali prima selamat, maka keluarga grup komputasional $\{\mathbb{Z}_N^* : N \in \mathcal{N}_k\}$ (dengan operasi hasil kali modulo dan prosedur sampling seragam atas QR_N) merupakan grup *pseudo-free* berkenaan dengan ensembel distribusi yang sama.

Bukti:

Misalkan $\mathbb{Z}_N^*$ tidak *pseudo-free*; dengan kata lain, ada algoritma probabilistik berwaktu polinomial $\mathcal{A}$ yang pada input acak $N \in \mathcal{N}_k$ dan elemen grup acak $\alpha : A \to \mathrm{QR}_N$, menghasilkan output persamaan yang tak terpenuhi $E : w_1 = w_2$ (atas konstanta A dan variabel X) bersama dengan solusi $\xi : X \to \mathbb{Z}_N^*$ milik E_α atas grup $\mathbb{Z}_N^*$. Akan digunakan $\mathcal{A}$ untuk menyelesaikan permasalahan QR-RSA kuat untuk distribusi yang sama. Yakni, diberikan secara acak $N \in \mathcal{N}_k$ dan $\gamma \in \mathrm{QR}_N$, kemudian dicari bilangan bulat $e > 1$ dan elemen grup $\xi \in \mathbb{Z}_N^*$ sedemikian hingga $\xi^e = \gamma$. Dengan menggunakan Teorema 2.5.9, hal ini juga mengakibatkan algoritma tersebut mampu menyelesaikan permasalahan RSA kuat standar. Algoritma $\mathcal{A}$ mula-mula akan mengecek

$g = \gcd(\gamma - 1, N)$. Kemudian akan dibagi menjadi 3 kasus:

1) jika $g = N$, maka $N | \gamma - 1$, dan $\gamma \equiv 1 (\bmod N)$. Jadi bisa langsung ditentukan output berupa solusi permasalahan QR-RSA kuat dengan input (N, γ), contoh: $(\xi, e) = (1,3)$.
2) jika $g \notin \{1, N\}$, maka $g \in \{P, Q\}$, dan dapat dengan mudah menghitung nilai $\phi(N)$ yaitu $\phi(N) = (g-1)\left(\frac{N}{g} - 1\right)$. Juga didapatkan output solusi $(\xi, e) = (\gamma, \phi(N) + 1)$ untuk permasalahan QR-RSA kuat (N, γ).
3) jika $g = 1$, maka dengan menggunakan Lemma 3.1, γ pembangun QR_N dan diproses sebagai berikut.

Akan digunakan γ untuk sampling $\alpha(a) \in \mathrm{QR}_N$. Untuk sebarang $a \in A$, pilih $v_a \in \{0, \ldots, N|A|K(k) - 1\}$ secara acak seragam untuk suatu fungsi super-polinomial $K(k) \geq k^c, \forall c \in \mathbb{N}$, dan tentukan $\alpha(a) = \gamma^{v_a}$. Dengan menggunakan Lemma 3.2, jarak statistik antara $\alpha(a)$ dan distribusi atas QR_N paling besar

$$\frac{|\mathrm{QR}_N|}{2N|A|K(k)} < \frac{|\mathrm{QR}_N|}{2\phi(N)|A|K(k)} = \frac{1}{8|A|K(k)} < \frac{1}{|A|K(k)} \leq \frac{1}{K(k)}$$

Karena nilai $\alpha(a)$ dipilih secara bebas, jarak antara α dan pengaitan terpilih seragam paling besar sebesar $\frac{1}{K(k)} \leq \frac{1}{k^c}, \forall c \in \mathbb{N}$. Ketika α berdistribusi normal, algoritma $\mathcal{A}$ berhasil dengan peluang yang tak terabaikan $\delta(k) \geq k^{-c_0}$ untuk suatu $c_0 \in \mathbb{N}$. Karena α berjarak kurang dari $\frac{1}{K(k)}$ dari distribusi normal, $\mathcal{A}$ berhasil dengan peluang $\delta(k) - \frac{1}{K(k)} > \frac{1}{k^{c_0}} - \frac{1}{k^c}$. Algoritma $\mathcal{A}$dengan peluang tersebut berhasil menghasilkan output persamaan $E: w_1 = w_2$ (atas variabel X dan konstanta A) yang tak terpenuhi atas $F(A)$. Untuk menyelesaikan permasalahan QR-RSA kuat, dengan menggunakan Lemma 3.3, persamaan $E: w_1 = w_2$ dan solusi ξ diubah menjadi persamaan satu peubah

$$E': x^e = \prod_{a \in A} a^{d_a}$$

yang tak terpenuhi atas grup bebas dengan

$$e = \gcd(e_x : x \in X)$$

dan solusinya

$$\xi'(x) = \prod_{x \in X} \xi(x)^{\frac{e_x}{e}}$$

atas $\mathbb{Z}_N^*$. Perhatikan bahwa persamaan E' terpenuhi (atas grup bebas) jika $e | \gcd(d_a : a \in A)$. Oleh karena itu, pastilah $e \nmid \gcd(d_a : a \in A)$. Perhatikan bahwa

$$(\xi')^e = \prod_{a \in A} \alpha(a)^{d_a} = \prod_{a \in A} (\gamma^{v_a})^{d_a} = \gamma^{\sum_a v_a d_a}$$

Berdasarkan nilai $\gcd(e, pq)$, dibagi 3 kasus:

1) jika $\gcd(e, pq) = pq$ dan $e \neq 0$, maka $pq | e$ dan bisa langsung dihasilkan output solusi $(\gamma, |e| + 1)$ untuk permasalahan QR-RSA kuat (N, γ) karena $o(\gamma) = pq$ sehingga $\gamma^{|e|+1} \equiv \gamma^{cpq+1} \equiv (\gamma^{pq})^c \gamma \equiv 1^c \cdot \gamma \equiv 1 \cdot \gamma \equiv \gamma (\bmod N)$. Meskipun pq tidak diketahui, namun pengecekan bisa dilakukan dengan cara mengecek apakah solusi $(\gamma, |e| + 1)$ valid. Cara serupa dilakukan untuk semua kasus berikutnya.
2) jika $\gcd(e, pq) \in \{p, q\}$, maka $o(\gamma^e) = \frac{pq}{\gcd(pq, e)} \in \{p, q\}$. Tentunya, γ^e bukan pembangun QR_N. Menurut Lemma 3.1, $\gcd(\gamma^e - 1, N) \neq 1$. Karena $\gamma^e \not\equiv 1 (\bmod N)$, juga berakibat $N \nmid (\gamma^e - 1)$ sehingga $\gcd(\gamma^e - 1, N) \neq N$. Oleh sebab itu, pastilah $g = \gcd(\gamma^e - 1, N) \in \{P, Q\}$. Sehingga dapat dengan mudah menghitung nilai $\phi(N)$ yaitu $\phi(N) = (g-1)\left(\frac{N}{g} - 1\right)$. Juga didapatkan output solusi $(\xi, e) = (\gamma, \phi(N) + 1)$ untuk permasalahan QR-RSA kuat (N, γ).
3) jika $e = 0$, dengan menggunakan Lemma 3.4, maka $d = \sum_a v_a d_a \neq 0$ terjadi dengan peluang paling besar $\frac{1}{4}$. Akibatnya, dengan peluang paling kecil $\frac{3}{4}$, $(\gamma, |d| + 1)$ adalah solusi permasalahan QR-RSA kuat (N, γ) karena $|d| + 1 > 1$ dan
$$\gamma^{|d|+1} \equiv \gamma \cdot \gamma^{|d|} \equiv \gamma \cdot (\xi')^0 \equiv \gamma (\bmod N).$$
4) jika $e \neq 0$ dan $\gcd(pq, e) = 1$, dari Lemma 3.5, maka diperoleh bahwa peluang $e \nmid d = \sum_a v_a d_a$ paling kecil $\frac{3}{8}$. Diproses sebagai berikut:

Misalkan $e' = \frac{e}{t}$ dan $d' = \frac{d}{t}$ dengan $t = \gcd(e, d)$. Dengan mengasumsikan $e \nmid d$ (yang terjadi dengan peluang paling sedikit $\frac{3}{8}$), diperoleh $t \neq e$, dan berakibat $e' > 1$. Perhatikan bahwa dari $\gcd(e, pq)$

dan $t|e$ diperoleh $\gcd(t, |\mathrm{QR}_N|) = 1$. Oleh sebab itu, kongruensi $(\xi')^e \equiv \gamma^d (\mathrm{mod}\, N)$ berakibat

$$(\xi')^{e't} \equiv \gamma^{d't} (\mathrm{mod}\, N)$$

$$(\xi')^{2e't} \equiv \gamma^{2d't} (\mathrm{mod}\, N)$$

karena kedua ruas residu kuadratik dan $\gcd(t, pq) = 1$, maka cukup untuk menyimpulkan bahwa

$$(\xi')^{2e'} \equiv \gamma^{2d'} (\mathrm{mod}\, N)$$

sehingga

$$N|\left((\xi')^{2e'} - \gamma^{2d'}\right)$$

$$N|\left((\xi')^{e'} + \gamma^{d'}\right)\left((\xi')^{e'} - \gamma^{d'}\right)$$

Jika $(\xi')^{e'} \neq \pm\gamma^{d'}$, maka $(\xi')^{e'} \pm \gamma^{d'} \neq 0$. Sehingga bisa dihitung faktorisasi $\{P, Q\} = \{\gcd\left(N, (\xi')^{e'} + \gamma^{d'}\right), \gcd\left(N, (\xi')^{e'} - \gamma^{d'}\right)\}$ dan $\phi(N) = (P-1)(Q-1)$. Sehingga dapat dihasilkan output solusi $(\gamma, \phi(N) + 1)$ untuk permasalahan QR-RSA kuat (N, γ). Kasus berikutnya terjadi jika $(\xi')^{e'} = \pm\gamma^{d'}$. Jika $(\xi')^{e'} = \gamma^{d'}$, maka dengan mengunakan algoritma Euclid yang diperluas, dicari bilangan bulat e'' dan d'' sedemikian hingga $e'e'' + d'd'' = \gcd(e', d') = 1$. Output solusinya adalah $\left((\xi')^{d''}\gamma^{e''}, e'\right)$ karena

$$\left((\xi')^{d''}\gamma^{e''}\right)^{e'} \equiv (\xi')^{e'd''}\gamma^{e'e''} \equiv \gamma^{d'd''}\gamma^{e'e''} \equiv \gamma (\mathrm{mod}\, N)$$

Jika $(\xi')^{e'} = -\gamma^{d'}$, maka e' haruslah ganjil agar $\left(-(\xi')\right)^{e'} = -(\xi')^{e'} = \gamma^{d'}$. Dengan begitu solusi untuk permasalahan QR-RSA kuat (N, γ) adalah $\left(\left(-(\xi')\right)^{d''}\gamma^{e''}, e'\right)$ karena

$$\left(\left(-(\xi')\right)^{d''}\gamma^{e''}\right)^{e'} \equiv \left(-(\xi')\right)^{e'd''}\gamma^{e'e''} \equiv \gamma^{d'd''}\gamma^{e'e''} \equiv \gamma (\mathrm{mod}\, N)$$

terbukti. □

KESIMPULAN

Keluarga grup komputasional $\{\mathbb{Z}_N^*: N \in \mathcal{N}_k\}$ (dengan operasi perkalian modulo dan prosedur sampling seragam atas QR_N) merupakan grup *pseudo-free* berkenaan dengan ensembel distribusi $\mathcal{N}$ atas hasil kali prima selamat di bawah asumsi RSA kuat. Beberapa *open problem* yang bisa diangkat sebagai riset lanjutan antara lain apakah $\mathbb{Z}_N^*$ juga *pseudo-free* bahkan jika N hasil kali bilangan prima sebarang atau ketika elemen γ diambil dari $\mathbb{Z}_N^*$ meskipun bukan residu kuadratik. Atau apakah bisa dibuktikan bahwa $\mathbb{Z}_N^*$ *pseudo-free* dengan mengasumsikan bahwa masalah RSA atau pemfaktoran N sulit diselesaikan.

DAFTAR PUSTAKA

[1] Buchmann, Johannes A.. 2000. *Introduction to Cryptography*. New York: Springer-Verlag New York, Inc..

[2] Cramer and Shoup. 2000. Signature schemes based on the strong RSA assumption. *ACM Transactions on Information and System Security*. 3(3):161–185, 2000. Preliminary version in CCS 1999.

[3] Fraleigh, John B.. 2000. *A First Course in Abstract Algebra*. Sixth Edition. Addison-Wesley Publishing Company, Inc.. USA.

[4] Gallian, Joseph. 2010. *Contemporary Abstract Algebra*. Toronto: D. C. Heath and Company.

[5] Goldreich, Oded. 2001. *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press.

[6] Menezes, Oorcshot, and Vanstone. 1996. *Handbook of Applied Cryptography*. CRC Press, Inc. USA.

[7] Micciancio, Daniel. 2008. The RSA group is pseudo-free. *Journal of Cryptology*. Volume 23. Issue 2. pp: 169-186.

[8] Papoulis, Athanasios. 2002. *Probability, Random Variables, and Stochastic Processes*. Fourth Edition. McGraw-Hill Companies, Inc.

[9] Rivest, Ronald L.. 2004. On the Notion of Pseudo-Free Groups. *Theory of Cryptography*. Volume 2951. pp: 505-521.

[10] Riyanto, Muhamad Zaki. 2007. *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Elgamal Atas Grup Pergandaan Zp**. Skripsi. Yogyakarta: Universitas Gadjah Mada.

[11] Rosen, Kenneth H.. 2003. *Discrete Mathematics and Its Applications*. Fifth Edition. AT&T Laboratories. USA.

[12] Rosen, Kenneth H.. 2000. *Elementary Number Theory and Its Applications*. Fourth Edition. AT&T Laboratories. USA.

[13] Stinson, D.R.. 1995. *Cryptography Theory and Practice*. Florida: CRC Press, Inc..