Kriptanalisis Linear Menggunakan Aproksimasi Ganda

Endah Wintarsih / 13501049
Jauharul Fuady / 13501066
Ridho Akhiro / 13501071

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11049@students.if.itb.ac.id , if11066@students.if.itb.ac.id, if11071@students.if.itb.ac.id

Abstrak

Kriptanalisis linear merupakan sebuah metode kriptanalisis yang cukup kuat yang dikemukakan oleh Matsui pada tahun 1992. Tipe dari kriptanalisis linear ini adalah *known plaintext attack*. Teknik ini telah digunakan untuk menyerang algoritma FEAL pada tahun 1992 dan algoritma DES pada tahun 1993. Kriptanalisis linear memungkinkan untuk menyerang algoritma blokcipher dan memungkinkan untuk mereduksi masukan yang diperlukan untuk membuat sebuah serangan yang sukses, namun masih memiliki sejumlah keterbatasan dalam hal-hal tersebut. Oleh karena itulah, linear cryptanalisis dengan menggunakan aproksimasi ganda dibuat oleh Kaliski dan Robshaw, sebagai perluasan dari teknik kriptanalisis linear yang dibuat oleh Matsui, untuk menanggulangi beberapa permasalahan yang belum pernah diperhitungkan. Selain itu keterbatasan kriptanalisis linear dalam menyerang algoritma DES juga merupakan faktor lain dibuatnya teknik kriptanalisis linear dengan menggunakan aproksimasi ganda.

***Kata kunci**: linear, cryptanalysis, aproksimasi ganda*

1. Pendahuluan

Teknik kriptanalisis linear diperkenalkan oleh Matsui dan Yamagishi pada tahun 1992 dalam sebuah penyerangan terhadap algoritma FEAL dan akhirnya diperbaiki oleh Matsui dan digunakan untuk menyerang algoritma DES pada acara EUROCRYPT di tahun 1993 [3]. Penyerangan terhadap algoritma DES tersebut memerlukan masukan 2^{47} pasangan plainteks/cipherteks yang diketahui [3] dan kemudian mengalami perbaikan sehingga masukan yang dibutuhkan hanya 2^{43} pasang [1].

Kriptanalisis linear mempelajari relasi statistik linear antara bit-bit dari plainteks, cipherteks dan kunci untuk pengenkripsian. Relasi tersebut digunakan untuk memprediksi nilai-nilai bit-bit kunci, dengan diketahui pasangan plainteks/cipherteks yang ada.[3]

Kajian dari makalah ini yaitu teknik kriptanalisis linear dengan menggunakan aproksimasi ganda dibuat oleh Kaliski dan Robshaw [1], sebagai pengembangan dari tkenik kriptanalisis linear dengan sebuah aproksimasi, untuk mengatasi beberapa kekurangan dari teknik kriptanalisis linear yang dibuat oleh Matsui.

Kriptanalisis linear dengan menggunakan aproksimasi ganda ini meningkatkan keefektifan dalam melakukan penyerangan terhadap algoritma DES, lebih dapat diterapkan, dan dapat mereduksi kebutuhan jumlah data masukan yang diperlukan untuk menyerang sebuah algoritma blokcipher dengan sangat efektif.

2. Ruang Lingkup

Makalah ini berisi kajian dari sejumlah literatur mengenai kriptanalisis linear dan kriptanalisis linear menggunakan aproksimasi ganda, namun terbatas hanya pada sebuah algoritma saja.

3. Kriptanalisis Linear

Ide dasar dari teknik kriptanalisis linear adalah untuk menemukan sejumlah aproksimasi linear ke dalam bentuk langkah iterasi blokcipher yang menghubungkan beberapa bit plainteks $P_{i1}...P_{ia,}$ cipherteks $C_{j1}...C_{ja,}$ dan kunci $K_{k1}...K_{ku}$ [1], dimana P_{in} merupakan bit paritas dari bit ke *i* pada plainteks P, C_{in} merupakan bit paritas dari bit ke *i* pada cipherteks C, dan K_{in} merupakan bit paritas dari bit ke *i* pada kunci K.

Untuk operasi-operasi linear sederhana seperti XOR dengan kunci atau sebuah permutasi dari bit-bit yang ada maka bisa didapatkan ekspresi linear yang memiliki probabilitas satu. Untuk elemen-elemen cipher yang bersifat non-linear seperti S-box, maka akan dicari aproksimasi linear dengan probabilitas *p* yang bernilai maksimum dari deviasi $|p-½|$. Aproksimasi untuk sebuah operasi di dalam enkripsi dapat didapatkan dengan mengkombinasikan kedua hal tersebut hingga menghasilkan sebuah aproksimasi untuk satu putaran dari enkripsi. [2]

Untuk seluruh operasi enkripsi, maka aproksimasi linear yang didapatkan adalah :

$$P[\chi_P] \oplus C[\chi_C] = K[\chi_K]. \quad (1)$$

Dimana $P[\chi_P]$ merepresentasikan $P_{i1}...P_{ia}$, $C[\chi_C]$ merepresentasikan $C_{i1}...C_{ia}$, dan $K[\chi_K]$ merepresentasikan $K_{i1}...K_{ia}$.

Jika persamaan 1 bernilai benar dengan probabilitas $p = ½ + Є$ untuk plainteks yang telah dipilih secara acak dan untuk kunci yang benar, maka hal tersebut dikatakan sebagai memiliki *bias* $Є$ [1].

Algoritma dasar yang memungkinkan seorang kriptanalis untuk mendapatkan satu bit informasi kunci dari sebuah aproksimasi linear adalah algoritma 1 [1].

Algoritma 1

Anggap persamaan 1 bernilai benar dengan nilai probabilitas $p = ½ + Є$.

Langkah 1. Anggap T sebagai jumlah pasangan plainteks/cipherteks sedemikian sehingga sisi kiri dari persamaan tersebut memiliki nilai sama dengan 0, dan anggap N adalah jumlah total dari seluruh pasangan yang ada.

Langkah 2. *If* (T > N/2)

- *then* ambil nilai $K[\chi_K] = 0$ (jika $Є > 0$) atau 1 (jika $Є < 0$)
- *else* ambil nilai $K[\chi_K] = 1$ (jika $Є > 0$) atau 0 (jika $Є < 0$)

4. Kriptanalisis Linear Menggunakan Aproksimasi Ganda

Apabila ada sebanyak *n* aproksimasi linear yang masing-masing mengandung bit kunci yang sama namun berbeda dalam hal penggunaan bit-bit plainteks dan cipherteks, maka dapat dianggap bahwa algoritma 1 di atas dapat digunakan pada aproksimasi linear

n yang manapun untuk menentukan statistik T_i , $1 \le i \le n$, dengan sejumlah nilai bias dan variansi.

Anggap bahwa aproksimasi linear ke-*i* untuk $1 \le i \le n$ adalah sebagai berikut [1]:

$$P[\chi^i_P] \oplus C[\chi^i_C] = K[\chi^i_K]. \quad (2)$$

Dengan mengasumsikan bahwa nilai tiap bias ϵ_i adalah positif.

Berikut ini adalah algoritma 1M [1] yang merupakan pengembangan dari algoritma 1 yang telah dibuat oleh Matsui.

Algoritma 1M

Langkah 1. Untuk $1 \le i \le n$, anggap T_i sebagai jumlah pasangan plainteks/cipherteks sedemikian sehingga sisi kiri dari persamaan 2 di atas bernilai sama dengan 0. Anggap N menyatakan jumlah total dari blok plainteks yang ada.

Langkah 2. Untuk sebuah himpunan beban $a_1,...,a_n$ dimana $\sum_{i=1}^{n} a_i = 1$ hitung

$$U = \sum_{i=1}^{n} a_i T_i, \quad (3)$$

Langkah 3. *If* U > N/2 *then* ambil nilai $K[\chi_K] = 0$, *else* ambil nilai $K[\chi_K] = 1$.

Analisis yang dilakukan oleh Kaliski dan Robshaw [1] di bawah ini menunjukkan keefektifan algoritma 1M dalam hal kebutuhan data masukan plainteks yang diketahui.

4.1 Asumsi-Asumsi yang Digunakan

Asumsi-asumsi yang digunakan dalam algoritma tersebut adalah : [1]

Asumsi 1. Untuk semua *i* dan *j* dengan nilai $i \ne j$, maka $x_i = x_j$ dengan nilai probabilitas ½, dimana nilai probabilitas tersebut diambil dari blok plainteks yang telah dipilih secara acak.

Asumsi 2. Pendistribusian nilai statistik dari persamaan 3 bisa dimodelkan dengan menggunakan pendistribusian normal secara akurat.

Selain asumsi-asumsi, teknik ini juga menggunakan sejumlah lemma yang tidak dikemukakan di makalah ini.

4.2 Penggunaan Algoritma 1M

Dalam pembuktian metode kriptanalisis linear menggunakan aproksimasi ganda, Kaliski dan Robshaw melakukan sejumlah percobaan penyerangan terhadap algoritma DES dengan versi jumlah putaran yang kecil.

Pemilihan algoritma DES dengan versi jumlah putaran yang kecil didasari pada keyakinan bahwa skala kecil tersebut cukup dapat menggambarkan bahwa teknik kriptanalisis linear dengan aproksimasi ganda tersebut juga dapat digunakan untuk penyerangan algoritma DES dengan jumlah putaran yang lebih besar.

Algoritma DES yang digunakan adalah versi dengan jumlah putaran sebanyak 5 (lima) kali dengan menggunakan dua aproksimasi linear yang digambarkan dengan -ACD- dan -DCA- sesuai dengan notasi yang digunakan oleh Matsui.

Masing-masing aproksimasi linear tersebut memiliki nilai bias $\epsilon = 25 \times 2^{-12} \approx 6{,}104 \times 10^{-3}$.

Jika K_i adalah 48 subkunci yang digunakan pada putaran ke-*i*, P_L adalah 32 bit awal dari blok plainteks, dan C_L adalah 32 bit

awal dari blok cipherteks, maka bisa didapatkan :

$P_1 : P_L[7, 18, 24, 29] \oplus C_L[7, 18, 24] = K_2[22] \oplus K_3[44] \oplus K_4[22]$

$P_2 : P_L[7, 18, 24] \oplus C_L[7, 18, 24, 29] = K_2[22] \oplus K_3[44] \oplus K_4[22]$

Untuk membuktikan bahwa asumsi 1 benar-benar dapat digunakan, Kaliski dan Robshaw menghitung keluaran yang dihasilkan dari masukan yang berupa 2.000.000 pasangan plainteks/cipherteks dan aproksimasi linear P_1 dan P_2. Karena hasil perhitungan dari kedua relasi menghasilkan bahwa keluaran dari kedua relasi tersebut menghasilkan kecocokan nilai sebanyak 999.351 kali dan mengalami ketidakcocokan sebanyak 1.000.649 kali, maka Kaliski dan Robshaw berpendapat bahwa asumsi 1 tersebut dapat digunakan. [1]

Percobaan kemudian dilakukan dengan menggunakan sejumlah pasangan plainteks/cipherteks dengan nilai yang semakin meningkat. Nilai tersebut dipilih sedemikian sehingga jumlah pasangan plainteks/cipherteks yang digunakan merupakan nilai-nilai yang bersesuaian dengan $\frac{1}{8}\epsilon^{-2}$, $\frac{1}{4}\epsilon^{-2}$, $\frac{1}{2}\epsilon^{-2}$ dan ϵ^{-2}.

Hasil dari percobaan yang dilakukan oleh Kaliski dan Robshaw terlihat di bawah ini, dimana tergambar tingkat kesuksesan dengan menggunakan sebuah aproksimasi linear dimana teknik yang dipakai adalah algoritma 1 dan dengan menggunakan dua buah aproksimasi linear yang menggunakan teknik algoritma 1M. Hasil percobaan juga dibandingkan dengan perhitungan teori yang telah dilakukan oleh Kaliski dan Robshaw.

Hasil percobaan :

Jumlah pasangan	3.356	6.711	13.422	26.844
P1	81%	86%	94%	99%
P2	75%	88%	92%	99%
Menggunakan P1 dan P2	92%	95%	98%	100%

Hasil perhitungan teori :

Jumlah pasangan	3.356	6.711	13.422	26.844
P1	76%	84%	92%	98%
P2	76%	84%	92%	98%
Menggunakan P1 dan P2	84%	92%	98%	100%

5. Kesimpulan

Kriptanalisis linear yang diperkenalkan oleh Matsui merupakan suatu metode kriptanalisis yang cukup efektif dalam melakukan penyerangan terhadap algoritma blokcipher seperti DES dan sebagainya.

Pengembangan kriptanalisis linear yang sebelumnya hanya menggunakan sebuah aproksimasi linear menjadi kriptnalisis linear yang menggunakan aproksimasi ganda menghasilkan hasil yang sangat baik yaitu dalam hal pereduksian informasi masukan yang dibutuhkan dalam melakukan penyerangan terhadap algoritma blokcipher.

Sesuai dengan hasil eksperimen yang telah dilakukan oleh Kaliski dan Robshaw, penggunaan teknik kriptanalisis linear dengan menggunakan aproksimasi ganda menghasilkan hasil yang sama dengan kriptanalisis linear yang menggunakan sebuah aproksimasi linear hanya dengan membutuhkan informasi masukan yang

berjumlah setengah dari informasi masukan yang diperlukan oleh teknik kriptanalisis linear yang menggunakan sebuah aproksimasi linear.

Hasil yang sangat baik ini diharapkan dapat menjadi pemicu pengembangan teknik kriptanalisis yang lain sehingga dapat digunakan untuk mengukur kekuatan suatu algoritma blokcipher yang akhirnya dapat dibuat sebuah algoritma blokcipher yang lebih kuat dalam menghadapi serangan-serangan yang dilakukan oleh pihak luar.

Daftar Pustaka

[1] B.S Kaliski Jr. and M.J.B. Robshaw, *Linear Cryptanalysis Using Multiple Approximations*, http://www.isg.rhul.ac.uk/~mrobshaw/publications/Crypto94.pdf, diakses tanggal 31 Desember 2004 pukul 12:17

[2] A. Biryukov and C. De Cannière, *Linear Cryptanalysis*, http://www.esat.kuleuven.ac.be/~abiryuko/Enc/e32.pdf, diakses tanggal 31 Desember 2004 pukul 12:17

[3] E. Biham, *On Matsui's Linear Cryptanalysis*, http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E94/341.pdf, diakses tanggal 7 Januari 2005 pukul 10:05

[4] T. Ritter, *Linear Cryptanalysis : A Literature Survey*, http://www.ciphersbyritter.com/RES/LINANA.HTM, diakses tanggal 31 Desember 2004 pukul 11:39