ANALISIS KETAHANAN ALGORITMA ENKRIPSI STANDAR *PERVASIVE COMPUTING* (CLEFIA) TERHADAP SERANGAN *LINEAR* DAN *DIFFERENTIAL CRYPTANALYSIS* DENGAN METODE *LAT*, *XOR TABLE* DAN *NONLINEARITY*

Amas
Lembaga Sandi Negara
Jl Harsono RM No.70, Ragunan, Ps.Minggu
Jakarta Selatan -12550
e-mail : amas@lemsaneg.go.id

Abstrak
Pervasive computing memiliki konsep bahwa komputasi bisa dimunculkan dimana saja, menyatu dalam aktifitas manusia dan dikembangkan dalam sumber daya ringan. Salah satu isu penting dalam pervasive computing adalah keamanan, yaitu bagaimana menerapkan fitur keamanan meskipun dengan sumber daya terbatas. CLEFIA merupakan algoritma block cipher yang menjadi standar dalam ISO/IEC 29192-2 untuk penerapan enkripsi simetrik pada perangkat dengan sumber daya ringan. Karakteristik tersebut sangat cocok untuk diimplementasikan pada teknologi berbasis pervasive computing. Sebagai algoritma kriptografis dalam mendukung keamanan, tentu harus memenuhi aspek kekuatan yang memadai. Salah satu kriteria penting pada algoritma kriptografi berbasis simetrik saat ini yaitu ketahanan terhadap linear dan differential cryptanalysis. Pada penelitian ini, penulis melakukan analisis terhadap salah satu komponen utama dalam algoritma CLEFIA, yaitu s-box. Beberapa metode yang digunakan yaitu LAT, XOR Table dan nonlinearity. Analisis ini digunakan untuk mengetahui ketahanan s-box yang digunakan terhadap linear dan differential cryptanalysis. Dari hasil analisis didapatkan s-box S0 memiliki nilai LAT maksimal sebesar 24, nilai differential uniformity sebesar 10 dan nilai nonlinearity 100. S-box S1 memiliki nilai LAT maksimal sebesar 16, nilai differential uniformity sebesar 4 dan nilai nonlinearity 112. Nilai tersebut menghasilkan probabilitas sukses yang sangat kecil untuk diberlakukan serangan linear dan differential cryptanalysis sehingga disimpulkan bahwa S-box CLEFIA tahan terhadap linear dan differential cryptanalysis.

***Kata Kunci** : CLEFIA, s-box, LAT, XOR Table, nonlinearity, linear cryptanalysis, differential cryptanalysis dan pervasive computing.*

1. PENDAHULUAN

Pervasive computing merupakan suatu konsep di dalam *software engineering* dan *computer science* bahwa komputasi bisa dimunculkan dimana saja. Berbeda dengan *desktop computing*, *pervasive* dapat terjadi dengan menggunakan perangkat apapun, didalam lokasi apapun dan dalam format apapun. Interaksi user dengan komputer bisa terjadi dalam berbagai bentuk, termasuk *laptop computers*, *tablet* dan terminal yang menyatu dengan obyek sehari-hari. Beberapa teknologi yang mengiringi perkembangan *pervasive computing* yaitu Internet, *advanced middleware*, *operating system*, *mobile code*, *sensors*, *microprocessors*, *networks*, *mobile protocols*, dan *location and positioning*.

Lingkungan yang didukung dengan teknologi ini dibuat untuk memudahkan semua pekerjaan manusia dalam mencapai tujuan atau kebutuhan hidupnya. Setiap teknologi yang mendukung *pervasive* ini dikembangkan dalam sumber daya yang murah dan dioptimasikan sesuai dengan tujuannya masing-masing. Integrasi dari keseluruhan teknologi ini memungkinkan manusia dapat menikmati setiap layanan teknologi secara terhubung antar satu sama lain. Setiap pekerjaan atau proses yang dibutuhkan akan menjadi lebih cepat dan efisien karena pekerjaan-pekerjaan tersebut sudah diproses secara otomatis.

Salah satu isu penting dalam *pervasive computing* adalah keamanan. Meskipun dengan sumber daya terbatas dalam setiap teknologi berbasis *hardware* ini tetap perlu jaminan keamanan. Misal, setiap data transaksi pribadi yang melalui perangkat berbasis *pervasive computing* tersebut harus terjamin kerahasiaannya. Hal ini tentu lebih dikhususkan lagi untuk penerapan di bidang tertentu seperti militer, perbankan dll. Oleh karena itu dibuatlah sebuah standar melalui ISO/IEC 29192-2 untuk enkripsi pada teknologi berbasis *hardware* dengan karakteristik tersebut seperti RFID, *smartcard*, sensor network dll.

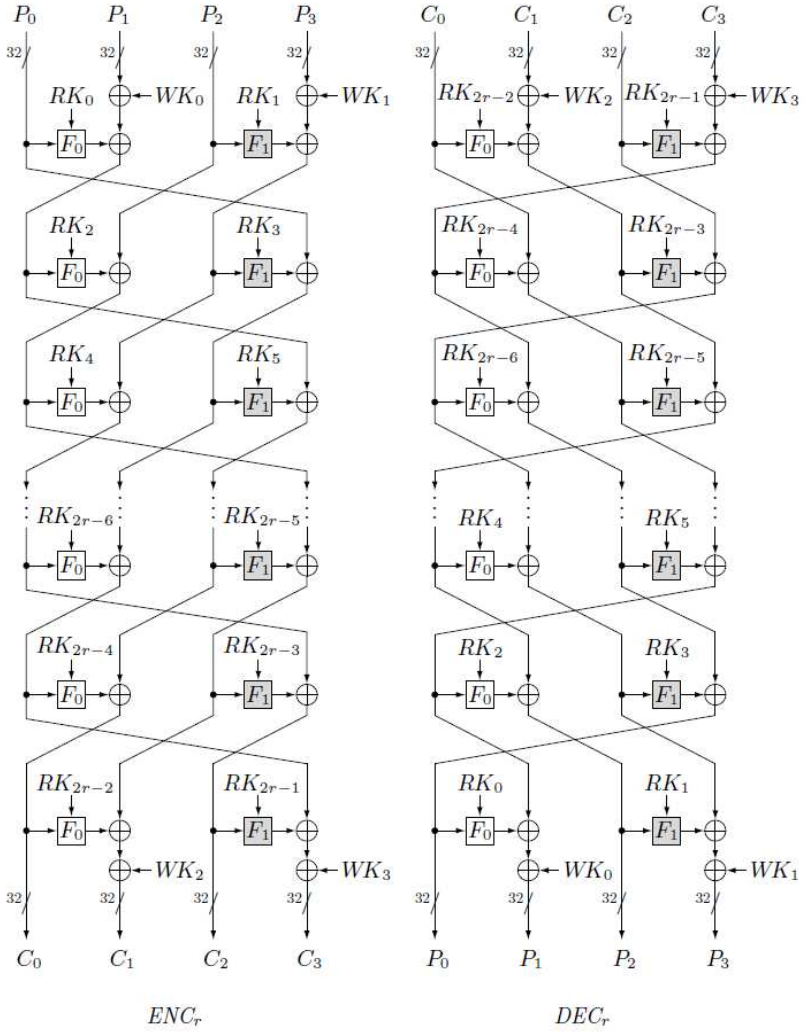
Salah satu algoritma enkripsi simetrik berbasis *block cipher* yang distandarkan sesuai ISO/IEC 29192-2 yaitu CLEFIA. Sebagai algoritma standar tentu harus memiliki kriteria kriptografis yang memadai, salah satunya

yaitu ketahanan *linear* dan *differential cryptanalysis*. Pada penelitian ini, penulis melakukan analisis terhadap salah satu komponen utama dalam algoritma CLEFIA, yaitu s-box. Beberapa metode analisis yang digunakan yaitu dengan *LAT*, *XOR Table* dan *Nonlinearity*. Dari hasil analisis ini kemudian kita menyimpulkan ketahanan s-box yang digunakan terhadap *linear* dan *differential cryptanalysis* berdasarkan metode tersebut.

2. LANDASAN TEORI

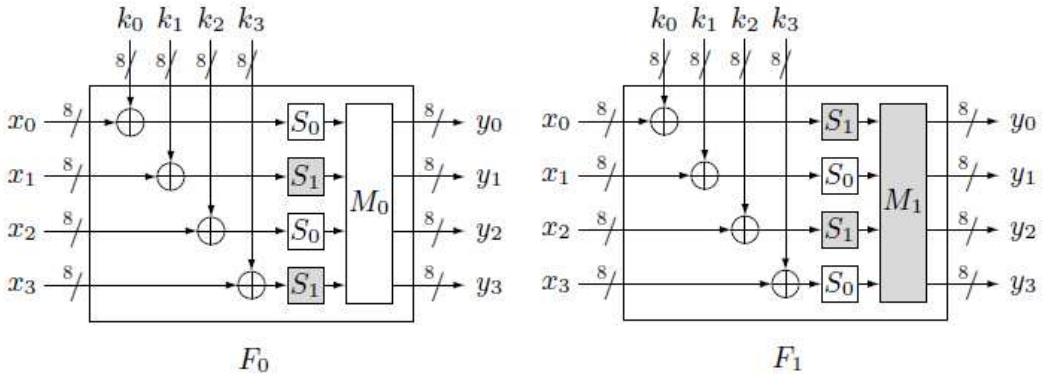
2.1. Algoritma CLEFIA (Sony Corp, 2007)

CLEFIA merupakan algoritma yang didesain atas dasar efisiensi namun tetap memperhatikan keamanan. Algoritma ini telah ditetapkan sebagai algoritma standar untuk *pervasive computing* yang memiliki kriteria untuk penerapan pada device yang memiliki sumberdaya terbatas melalui ISO/IEC 29192-2. Algoritma ini berbasis *block cipher* dengan ukuran 128 bit blok dengan variasi kunci 128, 192 dan 256 bit. CLEFIA menggunakan struktur Feistel yang membagi blok menjadi 4 jalur masing-masing berukuran 32 bit. Jumlah round pada CLEFIA bervariasi tergantung panjang kuncinya, untuk kunci 128 bit memiliki jumlah round 18, kunci 192 bit memiliki jumlah round 22 dan kunci 256 bit memiliki jumlah round 26. Diagram algoritma CLEFIA dapat dilihat pada gambar 1



Gambar 1 Diagram Algoritma CLEFIA

Fungsi F merupakan komponen utama dalam struktur algoritma CLEFIA yang berbasis Feistel. Didalamnya harus melibatkan operasi atau fungsi *nonlinear* dan memiliki sifat difusi yang maksimal. Fungsi F pada CLEFIA terdiri dari 3 komponen operasi yaitu operasi XOR dengan kunci, fungsi *nonlinear* S-box 8x8 dan fungsi *linear mixing*. Fungsi F pada CLEFIA dapat dilihat pada Gambar 2.



Gambar 2 Fungsi F pada CLEFIA

S0 dan S1 merupakan fungsi *nonlinear* S-box 8x8, sedangkan M0 dan M1 merupakan fungsi perkalian dengan matriks M0 dan M1 untuk proses *linear mixing*. Perkalian matriks M0 dan M1 ini didefinisikan berdasarkan pada polinomial primitive $z^8 + z^4 + z^3 + z + 1$ dengan menggunakan matriks M0 dan M1 berukuran 4 x 4 berikut :

$$M_0 = \begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 0x01 & 0x08 & 0x02 & 0x0a \\ 0x08 & 0x01 & 0x0a & 0x02 \\ 0x02 & 0x0a & 0x01 & 0x08 \\ 0x0a & 0x02 & 0x08 & 0x01 \end{pmatrix}$$

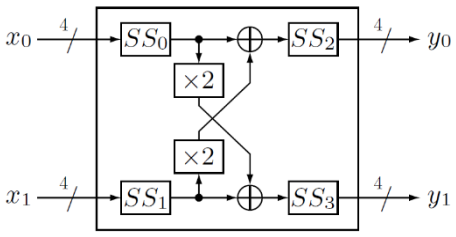
2.2. S-box CLEFIA (Sony Corp, 2007)

S-box nxn merupakan komponen utama dalam algoritma simetrik yang berisikan operasi substitusi dari n bit input menjadi n bit output. S-box nxn dapat didefinisikan sebagai fungsi pemetaan n bit input ke n bit output dan dapat dianggap sebagai n fungsi boolean. Terdapat beberapa kriteria untuk mendesain s-box yang berangkat dari prinsip konfusi dan difusi. Komponen ini didesain sedemikian sehingga kuat dalam menghadapi beberapa serangan kriptanalisis yang distandarkan. Dalam suatu algoritma biasanya s-box diimplementasikan dalam bentuk tabel.

S-box pada algoritma CLEFIA terdiri dari 2 buah S-box S0 dan S1 berukuran 8x8 bit. S0 dibangkitkan dengan mengkombinasikan 4 buat Sbox 4x4 yaitu SS0, SS1, SS2 dan SS3. Nilai dari S-box ini kemudian digunakan untuk mendefinisikan S0 dengan operasi sebagai berikut :

a. $t_0 \leftarrow SS_0(x_0), \quad t_1 \leftarrow SS_1(x_0), \quad$ dimana $x = x_0|x_1, \quad x_i \in \{0,1\}^4$
b. $u_0 \leftarrow t_0 \oplus 0x2 \cdot t_1, \quad u_1 \leftarrow 0x2 \cdot t_0 \oplus t_1$
c. $y_0 \leftarrow SS_2(x_0), \quad y_1 \leftarrow SS_3(x_0), \quad$ dimana $y = y_0|y_1, \quad y_i \in \{0,1\}^4$

Perkalian dengan *0x2* dalam $GF(2^4)$ yang didefinisikan pada polinomial primitive $z^4 + z + 1$. Untuk lebih jelasnya operasi untuk menghasilkan S0 dapat digambarkan seperti Gambar 3



Gambar 3. S0

S1 merupakan Sbox 8x8 yang didefinisikan sebagai berikut :

$$y = \begin{cases} g(f(x)^{-1}) & \text{jika } f(x) \neq 0 \\ g(0) & \text{jika } f(x) = 0 \end{cases}$$

Fungsi invers dibentuk dalam $GF(2^8)$ didefinisikan dalam polynomial $z^8 + z^4 + z^3 + z + 1$. Fungsi $f(.)$ dan $g(.)$ adalah transformasi affine pada $GF(2)$ dengan definisi sebagai berikut.

$$f: \begin{cases} \{0,1\}^8 \rightarrow \{0,1\}^8 \\ x_{(8)} \rightarrow y_{(8)} \end{cases}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

$$g: \begin{cases} \{0,1\}^8 \rightarrow \{0,1\}^8 \\ x_{(8)} \rightarrow y_{(8)} \end{cases}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Nilai x dan y didapatkan dari nilai $x_0|x_1|x_2|x_3|x_4|x_5|x_6|x_7$ dan $y_0|y_1|y_2|y_3|y_4|y_5|y_6|y_7$.

2.3. *Linear* dan *Differential cryptanalysis*

Linear dan *Differential cryptanalysis* merupakan serangan kriptanalisis yang tergolong dalam *known plaintext attack*. Jenis serangan ini membutuhkan sejumlah pasangan plainteks yang diketahui. Tujuan dari serangan ini yaitu penyerang dapat menemukan informasi tentang kunci dengan menggunakan sejumlah pasangan plainteks. Serangan ini menjadi salah satu standar keamanan dalam pengembangan algoritma simetrik saat ini, setelah berhasil diterapkan pada algoritma *Data Encrption Standard* (DES). Munculnya serangan *linear* dan *differential cryptanalysis* mengakibatkan algoritma DES sudah dianggap tidak aman dan kemudian digantikan dengan algoritma standar enkripsi baru melalui sebuah kompetisi. Melalui kompetisi tersebut lahirlah AES yang masih digunakan hingga saat ini.

Linear cryptanalysis adalah serangan yang berdasarkan pada aproksimasi hubungan *linear* yang efektif antara plainteks, cipherteks dan kunci (Matsui, 1994). *Differential cryptanalysis* adalah serangan yang menggunakan propagasi *differ* input dan *differ* output, yaitu karakteristik tentang XOR dari 2 input dengan XOR dari 2 output yang berkorespondensi (Biham & Shamir, 1991).

2.4. *Linear* Approximation Table (LAT)

LAT merupakan *tools* penting untuk mengukur keamanan dari suatu s-box terhadap serangan *linear cryptanalysis*. Distribusi LAT dari s-box didefinisikan sebagai jumlah semua variasi dari input x yang menyebabkan nilai operasi *dot product* antara input dengan α sama dengan nilai operasi *dot product* antara output dengan β. Misal input x dan output $S(x)$, maka LAT dinotasikan sebagai berikut (Akleylek & Yucel, 2007) :

$$\underset{\alpha,\beta \in F_2^n}{LAT(\alpha,\beta)} = \#\{x \mid \beta \cdot S(x) = \alpha \cdot x\} - 2^{n-1}$$

2.5. Exclusive Or (XOR) Table

XOR Table merupakan tools untuk memberikan informasi ketahanan s-box terhadap serangan *differential cryptanalysis*. XOR table dapat dikonstruksikan sebagai berikut (Akleylek & Yucel, 2007) :

$$XOR(dx,dy) = \#\{x \mid S(x) \oplus S(x \oplus dx) = dy\}$$

Dengan $dx = x' \oplus x''$ dan $dy = y' \oplus y''$ dimana y' merupakan output yang berkorespondensi untuk x'

2.6. *Nonlinearity*

Misal *An* merupakan himpunan fungsi *affine* pada F_2^n, maka yang disebut dengan *nonlinearity* suatu Fungsi Boolean f pada F_2^n merupakan jarak (*distance*) fungsi f terhadap himpunan *An* (fungsi *affine*). Dalam notasi matematikanya *nonlinearity* fungsi f didefinisikan

$$N_f = \min_l \{d(f,l)\}$$

dimana l merupakan sembarang fungsi *affine* (Meier, 1990).

Untuk mengukur nonlinearitas suatu fungsi dapat menggunakan *transformasi walsh.* Definisi kenonlinearitasan dengan menggunakan fungsi *walsh* yaitu sebagai berikut (Dundar, 2006) :

$$N_f = 2^{n-1} - \frac{1}{2} max_{\alpha \in F_2^n} \left| W_f(\alpha) \right|$$

Nilai *nonlinearity* maksimum (*perfect nonlinearity*) yang mungkin dari suatu Fungsi Boolean *f* memenuhi persamaan

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Nonlinearity dihitung untuk mengetahui ketahanan s-box terhadap serangan *linear cryptanalysis*. Semakin dekat *nonlinearity* s-box dengan nilai *perfect nonlinearity* maka semakin kuat terhadap serangan *linear cryptanalysis*.

3. METODE PENELITIAN

Metode Penelitian yang dilakukan pada penelitian ini adalah dengan studi literatur tentang algoritma CLEFIA, s-box CLEFIA, *Linear* dan *Differential cryptanalysis*, *LAT*, *XOR Table, Transformasi Walsh* dan *Nonlinearity*. Kemudian melakukan analisis terhadap komponen utama pada CLEFIA yaitu s-box dengan berdasarkan kriteria pada *LAT*, *XOR Table* dan *Nonlinearity* (lihat Bab 2). Pada uji *LAT* dan *XOR Table*, dilakukan penghitungan seperti pada Bab 2.4 dan Bab 2.5 untuk S0 dan S1 yang berukuran 8x8 sehingga untuk masing-masing s-box menghasilkan matriks berukuran 256x256. Matriks tersebut kemudian dianalisis sebaran dan nilai maksimalnya. Nilai maksimal ini menggambarkan ketahanan s-box terhadap *linear* dan *differential cryptanalysis*. Pada *nonlinearity* proses penghitungan dilakukan sesuai Bab 2.6 untuk semua fungsi boolean s-box dimana masing-masing s-box terdiri dari 8 fungsi boolean. *Nonlinearity* s-box merupakan nilai *nonlinearity* terkecil dari 8 fungsi boolean.

4. HASIL DAN PEMBAHASAN

4.1. Hasil Pengujian Distribusi *LAT*

Tabel *LAT* untuk masing-masing Sbox CLEFIA (S0 dan S1) berukuran 256x256 dimana elemen dihitung sesuai dengan rumus pada Bab 2.4. Penghitungan *LAT* menghasilkan nilai mutlak *LAT* untuk S0 yaitu antara 2 sampai 28, sedangkan untuk S1 yaitu antara 2 yaitu 16. Nilai maksimum *LAT* untuk S0 yaitu 24 dan untuk S1 yaitu 16. Berdasarkan nilai maksimal *LAT* tersebut, probabilitas bias terbaik untuk melakukan *linear cryptanalysis* pada S0 yaitu 3/32 ≈ 0,093 sedangkan untuk S1 yaitu 1/16 ≈ 0,062. Probablilitas ini masih terlalu kecil untuk dapat dilakukan *linear cryptanalysis* sehingga s-box S0 dan S1 masih dikatakan sulit untuk diterapkan *linear cryptnalysis.* Sebaran nilai elemen pada *LAT* untuk S0 dan S1 dapat dilihat pada Tabel 1.

Tabel 1 Persentase Distribusi nilai LAT S0 dan S1

Nilai Mutlak LAT	S0 (*%)	S1 (*%)
0	21,60	7,00
|2|	0	18,67
|4|	33,99	14,00
|6|	0	15,56
|8|	23,79	13,22
|10|	0	9,34
|12|	12,78	14,00
|14|	0	6,22
|16|	5,40	1,94
|18|	0	0
|20|	1,80	0
|22|	0	0
|24|	0,51	0

4.2. Hasil Pengujian *XOR Table*

XOR Table untuk masing-masing Sbox CLEFIA (S0 dan S1) berukuran 256x256 dimana elemen dihitung sesuai dengan rumus pada Bab 2.5. *Differential Uniformity* (nilai terbesar *XOR Table*) untuk S0 yaitu 10 sedangkan untuk S1 yaitu 4. Probabilitas terbaik untuk melakukan *differential cryptanalysis* pada S0 yaitu 5/128 ≈ 0,039 sedangkan pada S1 yaitu 1/64 ≈ 0,0156. Probablilitas ini masih terlalu kecil untuk dapat diterapkan *differential*

cryptanalysis sehingga s-box S0 dan S1 dianggap tahan terhadap *differential cryptanalysis.* Sebaran nilai *XOR Table* dapat dilihat pada Tabel 2

Tabel 2 Distribusi nilai XOR Table S0 dan S1

Nilai XOR Table	S0	S1
0	40021	33150
2	19501	32130
4	5037	255
6	848	0
8	119	0
10	9	0

4.3. Hasil Pengujian *Nonlinearity*

Proses penghitungan dilakukan sesuai Bab 2.6 untuk semua fungsi boolean s-box dimana masing-masing s-box terdiri dari 8 fungsi boolean. *Nonlinearity* s-box didefinisikan sebagai nilai *nonlinearity* minimum dari seluruh fungsi boolean pada s-box tersebut. Untuk s-box S0 didapatkan nilai *nonlinearity* sebesar 100, sedangkan S1 didapatkan nilai *nonlinearity* sebesar 112. Nilai *perfect nonlinearity* untuk sbox 8x8 sesuai dengan rumus pada Bab 2.6 yaitu 120, berdasarkan hasil tersebut disimpulkan bahwa S0 dan S1 mendekati *perfect nonlinearity* dengan nilai *nonlinearity* pada S0 < S1. Semakin dekat *nonlinearity*-nya dengan nilai sempurna maka semakin tahan terhadap *linear cryptanalysis*. Nilai *nonlinearity* per fungsi boolean masing-masing s-box S0 dan S1 dapat dilihat pada Tabel 3.

Tabel 3 *Nonlinearity* fungsi boolean (8) S0 dan S1

Nonlinearity boolean (f_i)	S0	S1
f_1	104	112
f_2	104	112
f_3	104	112
f_4	104	112
f_5	108	112
f_6	100	112
f_5	104	112
f_7	100	112

5. KESIMPULAN

Analisis terhadap s-box memiliki peranan penting dalam mengetahui ketahanan suatu algoritma terhadap *linear* dan *differential cryptanalysis*. Penyerang selalu berangkat dari kriteria s-box saat melakukan serangan *linear* dan *differential cryptanalysis* terhadap keseluruhan algoritma. Saat probabilitas sukses sangat kecil, maka tentunya mengakibatkan probabilitas sukses penyerang melakukan serangan *linear* dan *differential cryptanalysis* terhadap algoritma secara keseluruhan sangat kecil. Hasil penghitungan menunjukkan bahwa s-box S0 dan S1 berukuran 8x8 pada CLEFIA memiliki ketahanan terhadap *linear* dan *differential cryptanalysis* berdasarkan penghitungan *LAT*, *XOR Table* dan nilai *nonlinearity*. Dari analisis didapatkan s-box S0 memiliki nilai *LAT* maksimal sebesar 24, nilai *differential uniformity* sebesar 10 dan nilai *nonlinearity* 100. S-box S1 memiliki nilai *LAT* maksimal sebesar 16, nilai *differential uniformity* sebesar 4 dan nilai *nonlinearity* 112. Nilai tersebut menghasilkan probabilitas sukses yang sangat kecil untuk diberlakukan serangan *linear* dan *differential cryptanalysis.* S-box S1 pada CLEFIA lebih kuat secara kriptografis dibandingkan S0 berdasarkan pada kriteria *LAT*, *XOR Table* dan *nonlinearity*. Metode pembangkitan s-box pada S1 dapat dikatakan lebih baik berdasarkan kriteria kriptografis tersebut dibandingkan dengan metode pembangkitan s-box pada S0.

DAFTAR PUSTAKA

Akleylek, Sedat & Yucel, Melek. 2007. Comparing Substitution Boxes of the Third Generation GSM and Advanced Encryption Standard Ciphers, pp 157-162 : Turkey

Dundar, Baha Guclu, 2006. Cryptographic Properties of Some Highly Nonlinear Balanced Boolean Functions, Department of Cryptography-Ocak : Turkey

E. Biham & A. Shamir, 1991. "Differential Cryptanalysis of DES-Like Cryptosystems," Journal of Cryptology, volume:4 pp. 3-72 : Norway

M. Matsui, 1994. Linear Cryptanalysis Method for DES cipher, Lectures Notes in Computer Science no. 765, Springer Verlag, pp. 386-397 : Japan

Meier, Willy & Staffelbach Othmar, 1990. Nonlinearity Criteria for Cryptgraphic Function, Springer-Verlag: Switzerland

Sony Corporation, 2007. The 128-bit Blockcipher CLEFIA : Japan