TRANSFORMASI WALSH UNTUK ANALISIS KETIDAKLINEARAN FUNGSI BOOLEAN PADA KEAMANAN BLOCK CIPHER

Yusuf Kurniawan
Universitas Pasundan Bandung
Jalan Setiabudi 193 Bandung; e-mail: ysfk2002@yahoo.com

ABSTRAKSI

Keamanan kotak subtitusi sangat menentukan keamanan algoritma enkripsi block cipher. Keamanan kotak subtitusi dapat diukur dengan menghitung ketidaklinearan fungsi booleannya .Makalah ini akan membahas transformasi Walsh Hadamard yang dapat digunakan untuk menghitung ketidaklinearan kotak subtitusi. Analisis Linear Approximation Table (LAT) juga akan diberikan untuk memberikan perbandingan dengan hasil transformasi Walsh Hadamard.

Kata kunci: *Keamanan, kotak subtitusi, transformasi Walsh, LAT, block cipher.*

1. PENDAHULUAN

Analisis sandi linear merupakan salah satu metode terbaik untuk memecahkan algoritma enkripsi block cipher. Analisis sandi ini dapat memecahkan DES menggunakan 2^{43} *plaintext* yang diketahui.

Analisis sandi linear bekerja dengan mengeksploitasi kelinearan fungsi enkripsi. Semakin linear, semakin mudah analisis sandi ini berkerja. Analisis sandi berusaha mendapatkan pendekatan linear dalam bentuk [1]:

$$\left[\bigoplus_{\alpha=1}^{u} X_{i_\alpha}\right] \square \left[\bigoplus_{\beta=1}^{v} Y_{j_\beta}\right] = \left[\bigoplus_{\gamma=1}^{w} K_{k_\gamma}\right] \qquad (1)$$

dengan peluang sebesar mungkin. Misalkan peluang persamaan (1) disebut sebagai P_L, maka jika magnitude $|P_L - 1/2|$ cukup besar dan sejumlah besar pasangan plaintext-ciphertext yang diketahui tersedia, satu bit kunci ekivalen yang dinyatakan dengan penjumlahan bit-bit kunci di sebelah kanan pada persamaan (1) dapat ditentukan sebagai nilai yang paling sering muncul dan memenuhi persamaan (1).

Persamaan linear diturunkan dengan mengkombinasikan sejumlah pendekatan linear sejumlah kotak subtitusi dari beberapa ronde dengan mengusahakan agar suku-suku antara (suku yang bukan berasal dari plaintext, ciphertext, dan kunci) dihilangkan. Misalkan terdapat pendekatan linear terbaik dari sebuah kotak subtitusi dengan peluang p_l, maka jika jumlah pendekatan linear yang dikombinasikan untuk menghasilkan ekspresi keseluruhan adalah α, dapat ditunjukkan bahwa [1]:

$$|p_L - 1/2| \le 2^{\alpha-1} |p_l - \tfrac{1}{2}|^{\alpha} \qquad (2)$$

Ketidaklinearan dapat diukur berdasarkan pada jarak hamming terhadap fungsi affine terdekat. Fungsi affine m-bit didefinisikan sebagai fungsi yang memiliki bentuk

$$f(x) = a_0 \oplus a_1 X_1 \oplus \ldots \oplus a_m X_m + c \qquad (3)$$

di mana $X = [X_1 \ldots X_m]$ menyatakan masukan m-bit dan $a_i \in \{0,1\}$, $0 \le i < m$. Bila c=0, fungsi tersebut disebut sebagai fungsi linear.

Jarak antara dua fungsi m-bit f dan g dapat dinyatakan sebagai:

$$d(f,g) = \sum_{X \in \{0,1\}^m} [f(X) \oplus g(X)] \qquad (4)$$

Ketidaklinearan fungsi boolean m-bit, f, didefinisikan sebagai:

$$N(f) = \min_{g \in L} d(f,g) \qquad (5)$$

di mana L adalah seluruh fungsi boolean affine m-bit. Ketidaklinearan kotak subtitusi S m x n, didefinisikan sebagai ketidaklinearan minimum terhadap seluruh kombinasi linear tidak nol fungsi keluaran kotak subtitusi.

$$N(S) = \min_{a_1,\ldots a_n \in \{0,1\}, \text{semua } a_i \ne 0} N(\bigoplus_{i=1}^{n} a_i f_i) \qquad (6)$$

di mana fi menyatakan fungsi m-bit dari bit keluaran ke-i kotak subtitusi.

Secara ringkas dapat dikatakan bahwa ketidaklinearan fungsi f adalah jarak fungsi f terhadap semua kemungkinan fungsi linear (affine), sedangkan analisis sandi linear berusaha mencari pendekatan linear dari fungsi yang tidak linear. Semakin tidak linear sebuah fungsi, semakin sulit dicari pendekatan linearnya.

2. TRANSFORMASI WALSH HADAMARD

Fungsi walsh hadamard [5] merupakan salah satu tool kriptografi yang bermanfaat untuk memeriksa fungsi boolean. Bagian ini membahas transformasi ini untuk menghitung ketidaklinearan fungsi boolean. Transformasi Walsh terhadap fungsi f, $W_f : F_2^n \rightarrow Z$ didefinisikan sebagai:

$$W_f(a) = \sum_{x \in F_2^n} f(x)(-1)^{a.x} \qquad (7)$$

Karena kadang kala diinginkan menggunakan nilai real f dalam rentang [-1,1], maka didefinisikan fungsi sign yaitu:

$$\hat{f}(x) = (-1)^{f(x)} = 1 - 2f(x) \quad (8)$$

Sehingga transformasi Walsh terhadap $\hat{f}$ menjadi

$$W_{\hat{f}}(a) = \sum_{x \in F_2^n} \hat{f}(x)(-1)^{a.x}$$
$$= \sum_{x \in F_2^n} (-1)^{f(x) \oplus a.x} \quad (9)$$

Transformasi Walsh secara langsung berhubungan dengan jarak antar fungsi boolean terhadap fungsi-fungsi affine. Ambil $f : F_2^n \longrightarrow F_2$ dan $l(x) = a.x \oplus c$ adalah fungsi affine, di mana $a \in F_2^n$ dan $c \in F_2$.

Maka

$$d(f,l) = 2^{n-1} - \frac{(-1)^c}{2} W_{\hat{f}}(a) \quad (10)$$

Suku $(-1)^c W_{\hat{f}}(a)$ disebut sebagai jarak Walsh f ke l. Bila n genap, maka fungsi akan dapat memiliki jarak terjauh dari fungsi-fungsi affine. Fungsi semacam ini disebut sebagai fungsi Bent.

Fungsi boolean $f : F_2^n \rightarrow F_2$ disebut Bent jika

$$W_{\hat{f}}(a) = \pm 2^{n/2} \quad (11)$$

untuk semua a $\in F_2^n$

Ketidaklinearan fungsi f, $N(f)$ adalah jarak minimum f ke seluruh fungsi affine dapat dihitung menggunakan transformasi Walsh sebagai berikut:

$$N(f) = 2^{n-1} - \frac{1}{2} maks_{a \in F_2^n} \{|W_{\hat{f}}(a)|\} \quad (12)$$

N(f) akan memiliki nilai maksimum jika dan hanya jika f adalah fungsi bent. Ketidaklinearan fungsi affine adalah nol.

Matrik Hadamard H dengan orde 2^n adalah matrik 2^n x 2^n dengan komponen +1 dan -1 sedemikian sehingga

$$HH^T = 2^n I \quad (13)$$

Isi matrik ini ekivalen dengan fungsi affine, sehingga dapat digunakan untuk mengukur ketidaklinearan sebuah fungsi.

Dari persamaan (8) dapat dihitung perkalian dalam antara dua fungsi f dan g sebagai berikut :

$$\langle \hat{f}, \hat{g} \rangle = \sum_{x \in F_2^n} (-1)^{(f+g)(x)} \quad (14)$$
$$= 2^n - 2w(f+g)$$

di mana w adalah bobot hamming. Dan karena $w(f+g) = d(f, g)$ maka $\langle \hat{f}, \hat{g} \rangle = 2^n - 2\, d(f, g)$ atau

$$d(f, g) = 2^{n-1} - \tfrac{1}{2} \langle \hat{f}, \hat{g} \rangle \quad (15)$$

Sekarang kita akan menghitung nilai maksimal ketidaklinearan fungsi boolean menggunakan matrik Sylvester-Hadamard.

Misalkan $H_n = \begin{bmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^n-1} \end{bmatrix}$ (16)

di mana l_i menyatakan baris matrik ke-i dengan i = 1,2,….2^n-1. Karena H_n adalah matrik simetri, dan dengan persamaan (12) kita memiliki

$$\hat{f}.H_n = (\langle \hat{f}, l_0 \rangle, \langle \hat{f}, l_1 \rangle, ... \langle \hat{f}, l_{2^n-1} \rangle) \quad (17)$$

$$(\hat{f}.H_n)(\hat{f}.H_n)^T = H_n.H_n^T\, \hat{f}.\hat{f}^T$$
$$= 2^n\, \hat{f}.\hat{f}^T = 2^{2n} \quad (18)$$

Dengan menghitung sisi kiri persamaan (18) menggunakan (17) akan diperoleh:

$$(\hat{f}.H_n)(\hat{f}.H_n)^T = \sum_{a=0}^{2^n-1} \langle \hat{f}, l_a \rangle^2$$

Dan dengan mengkombinasikan hasil hasil tersebut, maka akan didapatkan

$$\sum_{a=0}^{2^n-1} \langle \hat{f}, l_a \rangle^2 = 2^{2n} \quad (19)$$

Dari persamaan (19) akan terdapat sebuah nilai a_i yang memenuhi $0 \le a_i \le 2^n$-1 sedemikian sehingga $\langle \hat{f}, l_{a_i} \rangle^2 \ge 2^n$. Ini berarti $\langle \hat{f}, l_{a_i} \rangle \ge 2^{n/2}$ atau $\langle \hat{f}, l_{a_i} \rangle \le -2^{n/2}$

Dari persamaan (15) dan $\langle \hat{f}, l_{a_i} \rangle \ge 2^{n/2}$ dapat diketahui bahwa $d(f,g) \le 2^{n-1} - 2^{\frac{n}{2}-1}$ di mana f adalah fungsi yang diperiksa dan g adalah semua fungsi affine yang mungkin ada. Bila $\langle \hat{f}, l_{a_i} \rangle \le -2^{n/2}$ benar, maka $\langle \hat{f}, -l_{a_i} \rangle = \langle \hat{f}, l_{a_i + 2^n} \rangle \ge 2^{n/2}$ di mana $l_{a_i+2^n} = -l_{a_i}$. Dan dari persamaan (15) diperoleh $d(f, g_{a_i}) = d(f, g_{a_i+2^n}) \le 2^{n-1} - 2^{\frac{n}{2}-1}$.

Dengan a_i, nilai $\langle \hat{f}, l_{a_i} \rangle$ dan $\langle \hat{f}, -l_{a_i} \rangle$ mencapai maksimal, sehingga $d(f, g)$ mencapai minimal, yang berarti bahwa ketidaklinearan maksimum adalah $2^{n-1} - 2^{\frac{n}{2}-1}$.

3. PERHITUNGAN WALSH DAN LAT

Pada bagian ini dibahas tentang perhitungan transformasi Walsh dan LAT [6] pada kotak subtitusi yang digunakan BC2 [2], yang berasal dari Camellia [4] dan hierocrypt [7]. Kotak subtitusi ini menggunakan fungsi yang ekivalen dengan fungsi

inversi. Menggunakan persamaan (9), dengan komputer pribadi, dapat dihitung deretan transformasi Walsh untuk f_0 sebagai berikut:

Tabel 1. Deret Transformasi Walsh f_0 pada Sbox Camellia

0	12	16	12	-16	-28	-8	12	-4	8	28	8	-20	0	-12	-8
-24	-4	16	-28	16	12	-16	-4	-28	-24	-4	16	-20	24	12	-8
0	-20	-24	-28	-16	4	0	-12	-28	0	-4	24	4	8	-12	-24
8	12	24	-4	0	-20	24	20	28	-32	-4	-16	4	16	-4	8
28	-8	-28	0	-20	16	-20	0	0	-20	24	-12	16	4	16	4
4	8	20	-24	12	24	-12	32	-8	-4	24	-4	0	-20	8	4
-4	8	-4	-24	-4	16	4	8	-8	4	-24	4	-24	28	16	4
4	8	-4	-16	12	24	12	-8	0	20	-24	-4	24	-12	24	4
-20	0	-4	16	-12	-16	12	24	-24	12	8	-4	-16	-4	-24	-12
4	-16	12	8	20	8	4	-8	16	-4	8	-12	-32	-12	-16	20
12	-16	20	-8	20	32	20	16	16	-12	-24	28	8	-12	-24	-12
20	0	4	0	20	8	-4	16	-8	-12	24	20	8	12	16	4
0	-12	8	-20	24	-12	8	-28	4	24	-4	16	28	-8	12	24
-24	20	24	4	-24	28	0	-28	-20	-24	12	-8	12	16	4	8
16	4	16	-12	24	-12	16	12	12	16	-4	0	4	-16	-4	-8
-24	4	32	-4	8	-20	24	12	-12	-16	28	8	4	-24	-12	-8

Tabel 2. Deret Transformasi Walsh f_0 pada Sbox Hierocrypt

0	-8	0	0	12	20	28	-4	20	12	28	12	-16	24	-24	24
28	12	-12	-4	0	16	-8	-16	8	-8	-24	0	12	-4	-20	20
-4	20	-12	4	16	-24	-8	24	-24	16	24	8	28	4	-4	-4
0	16	-16	8	-20	12	-4	-12	-12	-12	-4	-12	-16	0	24	-16
20	20	12	-12	-8	24	16	8	0	16	-16	24	20	4	4	-4
-24	-16	-8	24	-28	-4	-28	4	-4	20	4	4	-8	32	16	16
16	-16	-16	-24	-4	-20	-4	-12	20	-12	-4	4	0	16	8	-16
-4	4	-12	4	0	8	8	8	24	0	-8	24	12	20	-4	-20
-4	-4	4	-20	24	24	-16	-24	8	8	8	32	-12	20	4	12
-24	0	-8	8	12	-12	28	12	12	4	-12	-12	-16	24	24	24
8	8	8	0	-20	-4	-4	20	12	-4	-12	-20	16	16	-24	0
12	4	20	20	24	-16	0	-16	-8	32	-24	8	-12	-4	-28	-12
-8	-16	-8	-8	28	-28	-4	-4	-4	-28	-28	4	16	8	24	-8
-4	-4	-28	28	-24	-24	32	8	-24	-8	24	-16	-12	4	-12	-4
-12	-20	-4	12	32	-8	-24	8	-16	-24	-16	16	28	20	-4	12
0	0	16	24	20	-28	-12	-4	-12	-12	-4	-12	24	8	16	-24

Tabel 3. Deret Transformasi Walsh f_0 pada Sbox acak

0	16	12	4	-8	-16	-12	20	0	0	20	-4	-16	8	-12	-12
-28	4	0	-8	-4	4	-8	-8	-28	-12	-8	32	-28	12	24	-8
8	-24	-4	-28	-8	-16	-4	-4	-24	-8	4	28	0	-8	-20	-20
-4	28	0	-8	-4	-12	32	16	28	-20	-8	-32	20	12	16	0
16	0	-20	4	-8	16	-12	-12	-16	-16	20	-4	16	8	20	-12
-4	12	-8	0	4	28	-16	32	-4	-4	16	8	12	-28	16	0
-8	8	12	-28	8	16	-4	12	-8	-8	-12	-4	-16	24	12	-4
4	4	-8	-16	4	28	8	-8	4	20	-16	-8	28	-12	24	8
-28	12	-8	24	-4	-20	16	24	-28	12	0	0	-12	-12	-16	-24
0	-8	4	4	24	-8	12	-12	16	8	12	-20	-16	-32	-4	20
12	-12	8	8	12	44	8	32	28	-28	-32	32	4	-12	-24	-16
24	0	4	-12	8	8	4	12	-8	0	28	12	0	16	20	12
-12	-4	8	-24	28	12	0	-24	4	12	0	0	36	4	16	8
-24	16	28	12	-16	0	4	-36	-24	-16	20	4	24	-8	4	12
12	4	24	8	12	-4	8	16	12	4	0	16	-12	-12	-8	-16
-32	8	12	-4	16	-16	28	4	-16	-8	20	4	24	-24	-4	-12

Tabel 4. Deret Transformasi Walsh f_6 pada Sbox acak

0	8	0	16	-8	-16	0	0	0	-8	8	-24	0	-8	0	0
28	-12	-4	12	-4	-12	4	-12	20	-20	12	-4	-4	4	-20	-20
-28	-4	-4	-20	28	-28	12	-52	-20	4	12	-4	-20	36	-12	4
16	-24	-8	-8	0	-8	0	0	-16	-8	16	0	8	-32	-16	-16
24	-8	-24	-16	0	-16	-8	16	-16	0	24	16	16	0	16	8
-20	-4	-20	-12	-4	-20	-28	12	12	-4	-12	28	-12	-44	20	12
20	-12	-4	20	-4	-20	-4	4	4	-28	4	-4	-28	4	12	4
-8	24	0	8	-8	-8	-8	0	16	0	32	24	8	8	0	8
4	20	-20	4	-28	-12	-28	-36	-28	4	-12	28	12	28	-28	-4
16	-16	-8	16	8	-8	8	16	-8	-8	24	16	-8	-8	0	-8
8	8	8	-32	40	-24	-16	8	0	0	8	0	-24	-8	8	-16
-12	-12	36	12	-4	12	20	12	20	4	-4	-12	4	20	4	-4
-28	12	28	-20	-12	-4	-28	-12	-4	-12	12	12	4	12	-4	12
8	0	16	0	-16	-8	16	-16	-8	-16	-24	-8	-8	-16	16	32
-16	-8	0	0	32	8	-8	24	-16	-8	-8	-8	24	16	-8	8
20	-4	36	-12	12	4	-28	4	12	4	4	-28	-4	20	-20	12

Dari tabel 2 dapat dihitung jumlah kuadrat dari deret tersebut. Dan ternyata hasilnya sesuai dengan teorema Parseval:

$$\sum_{\alpha \in F_2^n} W_{\hat{f}}(a)^2 = 2^{2n} = 65536. \qquad (20)$$

Kondisi ini berlaku bagi semua fungsi yang terdapat pada kotak subtitusi tersebut. Dari tabel – tabel tersebut terlihat bahwa fungsi yang ekivalen dengan fungsi inversi bukanlah merupakan fungsi Bent karena tidak memenuhi persamaan (11). Ketidaklinearan fungsi-fungsi ini adalah = 112, sesuai dengan teori $2^{n-1} – 2^{n/2}$ [3].

Dari tabel 1 dan 2 juga dapat dipahami bahwa jarak fungsi f_0 ke fungsi linear bervariasi. Nilai 0 menunjukkan bahwa fungsi tersebut berada pada jarak terjauh dari fungsi linear, sedangkan nilai 32 menunjukkan fungsi tersebut berada pada jarak terdekat dengan fungsi linear. Dari teorema Parseval terlihat bahwa suatu fungsi yang memiliki jarak berjauhan dengan sebuah fungsi linear akan dekat dengan fungsi linear yang lain pada saat bersamaan, seperti dapat dilihat juga pada tabel 1 dan 2. Artinya kita tidak dapat membuat fungsi yang letaknya berjauhan dari semua dari fungsi linear (affine). Jarak terjauh terdapat pada fungsi bent yang memiliki ketidaklinearan maksimum sebesar 120.

Sebagai perbandingan, pada tabel 3 diperlihatkan deretan transformasi Walsh terhadap kotak subtitusi acak. Terlihat bahwa fungsi f_0 memiliki jarak maksimum 44, yang berarti lebih dekat dengan fungsi linear (affine) daripada fungsi yang ekivalen dengan fungsi inversi. Fungsi ini memiliki ketidaklinearan sebesar 106.

Tabel 4 memperlihatkan deretan transformasi Walsh terhadap fungsi f_6 pada kotak subtitusi yang dipilih secara acak. Terlihat bahwa fungsi ini memiliki ketidaklinearan yang lebih rendah daripada pada tabel 3. Secara umum, kotak subtitusi yang dipilih secara acak akan memiliki sifat kriptografi yang kurang baik. Dengan kata lain, kotak subtitusi yang bergantung kunci juga akan memiliki sifat yang tidak baik, meskipun sifat ini akan tertutup karena perubahan isi kotak subtitusi yang terus menerus.

Untuk melakukan analisis sandi linear, diperlukan suatu tabel yang disebut sebagai LAT (*Linear Approximation Table*). LAT adalah tabel pendekatan linear yang digunakan untuk mencari pendekatan linear dari fungsi yang tidak linear. Berdasarkan percobaan dengan komputer pribadi dengan bahasa C diperoleh bahwa bias terbesar Camellia dan fungsi yang ekivalen dengan fungsi inversi adalah sebesar 16. Sementara itu, bias terbesar LAT kotak subtitusi yang menggunakan isian acak seringkali lebih besar dari pada 16. Sama seperti pada hasil transformasi Walsh, kotak

subtitusi acak cenderung memberikan sifat yang kurang baik dari sudut pandang kriptografi.

Tabel 5. Sebagian LAT Camellia

128	0	0	0	0	0	0	0	0	0
0	2	6	12	6	-8	-4	2	2	16	4
0	-8	6	14	-6	2	12	4	4	-8	-6
0	6	0	-14	8	-2	-12	6	10	0	6
0	12	-6	6	8	0	2	2	0	12	-6
0	-2	-12	-10	-6	-4	6	-12	-14	4	2
0	8	16	-8	2	-2	-10	-6	16	12	8
0	14	-2	-8	-12	-2	-2	-4	14	12	0
0	-2	-6	8	10	0	0	6	-4	-10	-2
0	0	-8	4	4	12	8	12	14	-2	2
0	10	-4	6	0	-6	4	-2	-8	10	-4
0	-8	-10	2	-6	2	-8	4	-2	-6	0
0	14	4	10	10	12	2	-12	-4	14	-8
0	-8	-10	2	8	-4	10	10	6	-2	8
0	6	6	4	0	10	14	8	-4	-6	2
0	4	-12	-12	6	6	10	-2	2	2	-6
0	12	2	6	-4	0	-2	-14	-8	4	2
0	14	-12	6	-2	-12	2	-12	2	-4	10

Tabel 5 memperlihatkan sebagian dari isi LAT Camellia. LAT kotak subtitusi n x n akan berisi 2^n x 2^n, yang berarti bahwa untuk Camellia akan berisi 2^{16} isian, sehingga di makalah ini tidak diperlihatkan keseluruhannya.

Nilai maksimal bias LAT fungsi yang ekivalen dengan fungsi inversi sama besarnya dengan nilai mutlak terbesar transformasi Walsh, yaitu sebesar 16. Akan tetapi hal ini tidak berlaku bagi fungsi acak yang lain.

4. RINGKASAN

Dari uraian di atas dapat disimpulkan hal-hal berikut:

5. Transformasi Walsh dapat digunakan untuk mengukur ketidaklinearan fungsi yang terdapat pada kotak subtitusi.
6. Ketidaklinearan dibatasi oleh teorema Parseval.
7. Kotak subtitusi yang berasal dari fungsi yang ekivalen dengan fungsi inversi memiliki bias LAT dan nilai $W_{\hat{f}}$ maksimal yang sama. Untuk fungsi acak, nilainya seringkali tidak sama
8. Dari perbandingan transformasi Walsh dan LAT terlihat bahwa semakin besar ketidaklinearan semakin sulit pula dilakukan analisis sandi linear.
9. Perhitungan transformasi Walsh terhadap kotak subtitusi n x n hanya membutuhkan 2^n isian, sementara perhitungan LAT membutuhkan 2^{2n} isian. Dengan demikian lebih mudah melakukan analisis dengan transformasi Walsh dibanding menggunakan LAT.
10. Kotak subtitusi yang acak cenderung memiliki sifat kriptografi yang tidak memuaskan, khususnya dalam menghadapi analisis sandi linear.

PUSTAKA

[1] Matsui, M., Linear Cryptanalysis Method for DES Cipher, *Advances in Cryptology-EUROCRYPT '93* (Lecture Notes in Computer Science no. 765), Springer-Verlag, pp. 386-397., 1994.

[2] Yusuf Kurniawan, et.al. The New Block Cipher: BC2. Sudah diterima dengan minor revision oleh *IJNS* (*International Journal of Network Security*), *http://ijns.nchu.edu.tw*, 2006.

[3] Nyberg, K., Differentially uniform mapping for Cryptography, *Advances in Cryptology, Proc. Eurocrypt'93, LNCS* 765, T. Helleseth, Ed., Springer-Verlag, pp 439-444, 1994.

[4] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moria, Junko Nakajima, Toshio Tokita, Camellia: A 128-Bit Block Cipher Suitable for Multiple Platform-Design and Analysis, *submitted to NESSIE*, 2000.

[5] F. J. MacWilliams and N. J. A. Sloane. 1978. *The Theory of Error-Correcting Codes*. Amsterdam, New York, Oxford: North-Holland.

[6] L. O'Connor. Properties of linear approximation tables. In B. Preneel, editor, *Fast Software Encryption, Lecture Notes in Computer Science 1008*, Springer Verlag, 1995.

[7] Toshiba Corporation, Specification on a Block Cipher: Hierocrypt–L1, *submitted to NESSIE*, 2001.