Distribusi *Difference* dari S-Box Berbasis Fungsi Balikan Pada GF(2^8)

Andriani Adi Lestari
Lembaga Sandi Negara
e-mail: aaltari@gmail.com

Nunik Yulianingsih
Lembaga Sandi Negara
e-mail: nunik.yulianingsih@lemsaneg.go.id

***Abstract**: Substitution-box (s-box) is a basic component of block cipher which performs a substitution. Two powerful cryptanalysis techniques applied to block ciphers are linear cryptanalysis and differential cryptanalysis. The resistance against differential cryptanalysis can be achieved by eliminating high-probability differential trails. We should choose an s-box where the maximum difference propagation probability is as small as possible to eliminating high-probability differential trails. Nyberg proposed a method to construct the $n \times n$ s-box by using the inverse mapping on a finite field $GF(2^n)$ then implements affine transformations on $GF(2)$. In this study, we generate 47.104 8×8 s-box according to Nyberg. The experimental results showed that s-boxes have the maximum difference propagation probability $\delta = 2^{-6}$ with the same frequency.*

Keywords: *block cipher, difference distribution table, finite field, substitution-box keyword.*

1. Pendahuluan

Block cipher adalah skema enkripsi atau dekripsi yang memproses blok *plaintext* menjadi blok *ciphertext* dengan ukuran yang sama [1]. Pada umumnya *block cipher* mengkombinasikan fungsi sederhana seperti substitusi dan permutasi. *Substitution-box* (s-box) merupakan salah satu komponen dasar pada *block cipher* yang digunakan untuk melakukan substitusi dan berfungsi untuk menyembunyikan hubungan antara kunci dengan *ciphertext*.

Suatu algoritma dikatakan aman jika tidak dapat diserang dengan serangan yang sudah diketahui [2]. Serangan yang umumnya dapat diterapkan pada *block cipher* yaitu *linear cryptanalysis, differential cryptanalysis,* dan *related-key attack. Differential cryptanalysis* adalah sebuah metode yang menganalisis pengaruh dari suatu nilai *difference* dalam pasangan-pasangan *plaintext* terhadap nilai *difference* pasangan-pasangan *ciphertext* yang dihasilkan [3]. *Differential cryptanalysis* dilakukan dengan mencari *differential trail* dengan peluang yang tinggi untuk melakukan ekstraksi kunci. Salah satu mekanisme untuk mengeliminasi *differential trail* dengan peluang yang

tinggi adalah memilih s-box yang memiliki peluang maksimum *difference* sekecil mungkin. Mekanisme tersebut memberikan kriteria yang jelas dalam memilih s-box.

Salah satu metode untuk mengkonstruksi s-box berukuran $n \times n$ adalah metode yang diajukan oleh Nyberg [4], yaitu membangkitkan s-box dengan menggunakan pemetaan $f(x) = x^{-1}$ pada *finite field* $\left(GF(2^n)\right)$. Pada makalah ini akan dibangkitkan s-box berukuran 8×8 pada *finite field* $GF(2^8)$ menggunakan metode Nyberg. Penelitian ini bertujuan untuk mengetahui apakah s-box yang dibangkitkan menggunakan metode Nyberg memiliki peluang maksimum *difference* sekecil mungkin berdasarkan distribusi *difference*-nya.

2. Data dan Metode

Pada bagian ini dijelaskan mengenai metode pembangkitan s-box, *difference distribution table* dan tahapan penelitian. Tahapan penelitian meliputi teknik pengambilan sampel, banyaknya sampel yang digunakan, analisis data.

1) Metode Pembangkitan S-box

Sebuah s-box berukuran $n \times m$ adalah sebuah fungsi pemetaan yang dinotasikan dengan $S: \{0,1\}^n \rightarrow \{0,1\}^m$. S-box S akan mentransformasi input berukuran n bit menjadi output berukuran m bit dengan m tidak harus sama dengan n. *Block cipher* umumnya menggunakan s-box yang tetap, seperti pada *Data Encryption Standard* (DES) [5] dan *Advanced Encryption Standard* (AES) [6]. Namun terdapat *block cipher* yang menggunakan s-box yang dibangkitkan secara dinamis berdasarkan kunci, seperti pada Twofish [7].

Banyak metode yang dapat diterapkan untuk membangkitkan sebuah s-box tetap. Salah satu metode untuk mengkonstruksi s-box tetap berukuran $n \times n$ dengan peluang maksimum *difference* $\delta = 2^{2-n}$ adalah metode yang diajukan oleh Nyberg [4], yaitu membangkitkan s-box dengan menggunakan pemetaan $f(x) = x^{-1}$ pada *finite field* $\left(GF(2^n)\right)$. Pemetaan tersebut masih menghasilkan nilai input dan output yang tetap pada s-box (*fixed point*) yaitu pada input 0 dan 1. Untuk mengatasi hal tersebut maka perlu diimplementasikan transformasi affine pada $GF(2)$, yaitu

$$y = \boldsymbol{A} \cdot x + b \tag{1}$$

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} & a_{04} & a_{05} & a_{06} & a_{07} \\ a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} \\ a_{20} & a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} \\ a_{30} & a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} & a_{37} \\ a_{40} & a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} & a_{47} \\ a_{50} & a_{51} & a_{52} & a_{53} & a_{54} & a_{55} & a_{56} & a_{57} \\ a_{60} & a_{61} & a_{62} & a_{63} & a_{64} & a_{65} & a_{66} & a_{67} \\ a_{70} & a_{71} & a_{72} & a_{73} & a_{74} & a_{75} & a_{76} & a_{77} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix}$$

Tabel 1. S-box pada Algoritma AES

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

S-box pada algoritma AES (Tabel 1) merupakan s-box 8×8 dibangkitkan berdasarkan metode Nyberg, yaitu :

- Hitung invers perkalian pada $GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$ dengan elemen $\{00\}$ dipetakan ke dirinya sendiri.
- Kemudian lakukan transformasi affine (pada $GF(2)$)

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

Parameter dalam mengkonstruksi s-box 8×8 dengan metode Nyberg adalah polinomial irredusibel $m(x)$ berderajat 8 yang digunakan untuk mendefinisikan $GF(2^8)$, matriks biner $\boldsymbol{A}$ berdimensi 8×8 dan vektor biner b berdimensi 8×1 untuk membentuk fungsi affine. Banyaknya polinomial irredusibel $m(x)$ berderajat 8 adalah 30 polinomial, yaitu 11b, 11d, 12b, 12d, 139, 13f, 14d, 15f 163, 165, 169, 171, 177, 17b, 187, 18b, 18d, 19f, 1a3, 1a9, 1b1, 1bd, 1c3, 1cf, 1d7, 1dd, 1e7, 1f3, 1f5, 1f9 (polinomial disajikan dalam representasi hexadesimal, misal 11b merupakan representasi hexadesimal dari $x^8 + x^4 + x^3 + x^1 + 1$). Banyaknya matriks biner $\boldsymbol{A}$ berdimensi 8×8 yang memiliki invers adalah $\left((2^8 - 1)(2^8 - 2)(2^8 - 2^2) \dots (2^8 - 2^7)\right) = 2^{62.21}$ dan banyaknya kemungkinan dari vektor biner b adalah 2^8. Oleh karena itu, banyaknya kemungkinan s-box yang dapat dibentuk berdasarkan metode ini adalah $30 \cdot 2^{62.21} \cdot 2^8 = 2^{75.12}$.

2) *Difference Distribution Table*

S-box sebagai komponen yang melakukan substitusi pada *block cipher* merupakan fungsi non linear. Oleh karena itu, jika XOR dari pasangan input (*input difference*) diketahui maka tidak dapat diketahui dengan pasti XOR dari pasangan output (*output difference*). Untuk suatu nilai *input difference* memungkinkan beberapa nilai *output difference* namun tidak semua nilai *output difference* muncul. Tabel yang menunjukkan distribusi dari *input difference* dan *output difference* untuk semua pasangan yang mungkin dari s-box disebut tabel XOR atau *Difference Distribution Table* (DDT) [3]. Misal x adalah *input* dari *s-box* S berukuran $n \times n$ dan Δx adalah *input difference* dengan $x, \Delta x \in Z_2^n$. $S(x)$ adalah *output* dari *s-box* S dengan *input* x, $S(x \oplus \Delta x)$ adalah *output* dari *s-box* S dengan *input* $x \oplus \Delta x$, dan Δy adalah *output difference*. DDT untuk *input difference* Δx dan *output difference* Δy adalah

$$DDT[\Delta x, \Delta y] = \#\{X | S(x \oplus \Delta x) \oplus S(x) = \Delta y\}. \quad (2)$$

Peluang maksimum *difference* dinotasikan dengan δ yaitu rasio antara nilai DDT maksimum dengan 2^n, atau

$$\delta = \max_{\Delta x, \Delta y}\{DDT[\Delta x, \Delta y]\} \cdot 2^{-n}. \quad (3)$$

Untuk n genap maka peluang maksimum *difference* terkecil adalah 2^{2-n} [8]. Sampai saat ini, s-box dengan peluang maksimum *difference* adalah 2^{1-n} untuk *n* genap masih menjadi permasalahan terbuka.

3) Tahapan Penelitian

Data pada makalah ini adalah s-box 8×8. S-box tersebut dibangkitkan sesuai dengan metode Nyberg. Karena keterbatasan waktu dan sumber daya maka penelitian dilakukan dengan mengambil sampel s-box 8×8 dan tidak dilakukan pada populasi s-box 8×8 yang dapat dikonstruksi menggunakan metode Nyberg. Parameter yang digunakan adalah 8 polinomial irredusibel $m(x)$ berderajat 8, 23 matriks biner $\boldsymbol{A}$, dan 256 vektor biner b (semua kemungkinan vektor biner b). Banyaknya sampel s-box 8×8 pada penelitian ini adalah $8 \times 23 \times 256 = 47.104$ s-box. Setiap s-box tersebut dihitung DDT-nya sesuai dengan (2) dan diamati nilai δ beserta frekuensi terjadinya nilai δ. Simulasi pembangkitan s-box dan perhitungan DDT dilakukan menggunakan bahasa pemrograman C, sedangkan pembangkitan matriks biner $\boldsymbol{A}$ yang memiliki balikan dilakukan menggunakan Maple.

3. Hasil dan Pembahasan

Berdasarkan hasil eksperimen diperoleh bahwa nilai-nilai yang muncul pada tabel DDT dari 47.104 s-box 8×8 adalah 0, 2, dan 4. Setiap nilai DDT muncul dengan frekuensi yang sama pada semua s-box. Tabel 2 menunjukkan frekuensi nilai DDT dari setiap s-box.

Tabel 2. Frekuensi Nilai DDT

Nilai DDT	Frekuensi
0	32640
2	32130
4	255

Sumber: data primer (2016)

Berdasarkan tabel tersebut dapat diketahui bahwa nilai DDT maksimum dari setiap s-box adalah 4. Karena nilai maksimum DDT dari setiap s-box adalah 4, maka peluang maksimum *difference*-nya adalah $\delta = 4 \cdot 2^{-8} = 2^{-6}$. Peluang maksimum *difference* terkecil yang diketahui untuk $n = 8$ adalah $2^{2-n} = 2^{2-8} = 2^{6}$. Oleh karena itu, s-box yang dibangkitkan berdasarkan metode Nyberg memiliki peluang maksimum *difference* terkecil.

Pada setiap s-box terdapat 255 pasangan $(\Delta x, \Delta y)$ yang memiliki 4 solusi untuk $S(x \oplus \Delta x) \oplus S(x) = \Delta y$ (dengan kata lain terdapat 4 nilai $x \in Z_2^8$ yang memenuhi $S(x \oplus \Delta x) \oplus S(x) = \Delta y$). Hasil eksperimen tersebut sesuai dengan proposisi yang diajukan oleh Nyberg [4], yaitu pada pemetaan balikan $\#\{X | S(x \oplus \Delta x) \oplus S(x) = \Delta y\} \leq 4$ dengan penjelasan sebagai berikut :

Jika $S(x) = x^{-1}$ pada $GF(2^8)$ dan operasi $\oplus$ merupakan operasi $+$ pada $GF(2^8)$ maka $S(x \oplus \Delta x) \oplus S(x) = \Delta y$ dapat dituliskan sebagai

$$(x + \Delta x)^{-1} + x^{-1} = \Delta y \tag{4}$$

Untuk $x \neq 0$ dan $x \neq \Delta x$, maka Pers. (4) akan ekivalen dengan

$$\Delta y \cdot x^2 + \Delta x \cdot \Delta y \cdot x + \Delta x = 0 \tag{5}$$

yang memiliki paling banyak dua solusi pada $GF(2^8)$. Jika antara $x = 0$ atau $x = \Delta x$ adalah solusi untuk (4), maka keduanya adalah solusi dan $\Delta y = \Delta x^{-1}$. Dalam kasus tersebut (5) ekivalen dengan

$$x^2 + \Delta x \cdot x + (\Delta x)^2 = 0 \tag{6}$$

yang memberikan dua solusi tambahan untuk (3).
Penyelesaian (6) pada $GF(2^8)$ dilakukan dengan mengkuadratkan (6) dan mensubtitusikan $x^2 = \Delta x \cdot x + (\Delta x)^2$ sehingga diperoleh

$$x(x^3 + (\Delta x)^3) = 0$$

yang akan memberikan 4 solusi pada $GF(2^8)$, yaitu $x = 0$, $x = \Delta x$, $x = (\Delta x)^{d+1}$, $x = (\Delta x)^{2d+1}$ dengan $d = \frac{2^8-1}{3}$.

Penggunaan transformasi affine hanya digunakan untuk menghindari adanya pemetaan dengan nilai yang tetap. Transformasi tersebut mengubah nilai Δy dari fungsi invers dengan peluang satu. Jika x adalah input dari transformasi affine yang merupakan invers pada $GF(2^n)$, maka output *difference* Δy dari transformasi affine untuk input *difference* Δx adalah

$$\begin{aligned} \Delta y &= (\boldsymbol{A} \cdot x + b) \oplus (\boldsymbol{A} \cdot (x \oplus \Delta x) + b) \\ &= \boldsymbol{A} \cdot x \oplus b \oplus \boldsymbol{A} \cdot (x \oplus \Delta x) \oplus b \\ &= \boldsymbol{A} \cdot x \oplus \boldsymbol{A} \cdot (x \oplus \Delta x) \oplus b \oplus b \\ &= \boldsymbol{A} \cdot x \oplus \boldsymbol{A} \cdot (x \oplus \Delta x) \\ &= \boldsymbol{A} \cdot (x \oplus x \oplus \Delta x) \\ &= \boldsymbol{A} \cdot (\Delta x) \end{aligned} \tag{7}$$

Berdasarkan (7) dapat dilihat bahwa output *difference* dari transformasi affine adalah hasil perkalian antara matriks $\boldsymbol{A}$ dengan input *difference*. Hal tersebut sesuai dengan hasil eksperimen, yaitu penggunaan transformasi affine yang berbeda tidak mengubah sebaran dari nilai DDT, dengan kata lain transformasi affine tidak mengubah karakteristik *differential* dari s-box

4. Simpulan dan Saran

Berdasarkan hasil eksperimen diperoleh bahwa 47.104 s-box 8×8 yang dibangkitkan menggunakan metode Nyberg memiliki nilai peluang maksimum *difference* $\delta = 2^{-6}$ dengan frekuensi 255, sehingga dapat disimpulkan bahwa s-box yang dibangkitkan menggunakan metode Nyberg memiliki peluang maksimum *difference* terkecil yang mungkin untuk n genap. Penggunaan transformasi affine yang berbeda tidak mengubah sebaran dari nilai DDT.

Daftar Pustaka

[1] W. Stallings, *Cryptography and Network Security: Principles and Practices*. 2005.

[2] L. R. Knudsen, "Block Ciphers," in *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA: Springer US, 2011, pp. 152–157.

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," 1990.

[4] K. Nyberg, "Differentially uniform mappings for cryptography," *Advances in Cryptology — EUROCRYPT '93*. pp. 55–64, 1994.

[5] H. Feistel, "Data Encryption Standard (DES)," *Fips Pub 46-3*, vol. 3, 1999.

[6] N. Fips, "197: Announcing the advanced encryption standard (AES)," ... *Technol. Lab. Natl. Inst. Stand. ...*, vol. 2009, pp. 8–12, 2001.

[7] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, and C. Hall, "Twofish : A 128-Bit Block Cipher," *NIST AES Propos.*, vol. 15, no. 1, pp. 1–27, 1998.

[8] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-chapuy, "On Almost Perfect Nonlinear Functions Over Fn," vol. 52, no. 9, pp. 4160–4170, 2006.