On the Security of Rijndael-like Structures against Differential and Linear Cryptanalysis

Sangwoo Park[1], Soo Hak Sung[2], Seongtaek Chee[1],
E-Joong Yoon[1], and Jongin Lim[3]

[1] National Security Research Institute, Korea,
{psw,chee,yej}@etri.re.kr
[2] Department of Applied Mathematics, Pai Chai University, Korea
sungsh@woonam.paichai.ac.kr
[3] Center for Information Security Technologies(CIST), Korea University, Korea
jilim@cist.korea.ac.kr

Abstract. Rijndael-like structure is a special case of SPN structure. The linear transformation of Rijndael-like structures consists of linear transformations of two types, the one is byte permutation π and the other is linear transformation $\theta = (\theta_1, \theta_2, \theta_3, \theta_4)$, where each of θ_i separately operates on each of the four columns of a state. Furthermore, π and θ have some interesting properties. In this paper, we present a new method for upper bounding the maximum differential probability and the maximum linear hull probability for Rijndael-like structures. By applying our method to Rijndael, we obtain that the maximum differential probability and the maximum linear hull probability for 4 rounds of Rijndael are bounded by 1.06×2^{-96}.

1 Introduction

SPN(Substitution and Permutation Network) structure is one of the most commonly used structure in block ciphers. SPN structure is based on Shannon's principles of confusion and diffusion [4] and these principles are implemented through the use of substitution and linear transformation, respectively.

Rijndael [7], Crypton [12, 13] and Square [6] are the block ciphers composed of SPN structures. They have a common point for the type of their linear transformations. Each of their linear transformations consists of linear transformations of two types, the one is byte permutation π and the other is linear transformation $\theta = (\theta_1, \theta_2, \theta_3, \theta_4)$, where each of θ_i separately operates on each of the four columns of a state. Furthermore, each of bytes of each column of $y = \pi(x)$ comes from each different column of x, and we can determine the branch number of each of θ_i. In this paper, we call such a SPN structure Rijndael-like structure.

The security of SPN structures against differential cryptanalysis [2, 3] and linear cryptanalysis [14] depends on the maximum differential probability and the maximum linear hull probability. In [11], Keliher *et al.* proposed a method for finding the upper bound on the maximum average linear hull probability for SPN structures. Application of their method to Rijndael yields an upper bound of 2^{-75} when 7 or more rounds are approximated. In [10], it was proposed that the improved upper bound on the maximum average linear hull probability for Rijndael when 9 or more rounds are approximated is 2^{-92}, corresponding to a lower bound on the data complexity of 2^{97}. This is based on completion of 43% of the computation. It is estimated that the running time to completion is 200,000 hours on a single Sun Ultra 5.

In this paper, we present a new method for upper bounding the maximum differential probability and the maximum linear hull probability for Rijndael-like structures. We prove that the maximum differential probability for 4 rounds of Rijndael-like structures is bounded by $4p^{19} + 6p^{18} + 4p^{17} + p^{16}$, when the maximum differential probability for S-boxes is $p(\leq 2^{-3})$. Also, we prove that the maximum linear hull probability for 4 rounds of Rijndael-like structures is bounded by $4q^{19} + 6q^{18} + 4q^{17} + q^{16}$, when the maximum linear hull probability for S-boxes is $q(\leq 2^{-3})$. By applying our method to Rijndael, we obtain that the maximum differential probability and the maximum linear hull probability for 4 rounds of Rijndael are bounded by 1.06×2^{-96}.

2 SPN structures

One round of SPN structures generally consists of three layers of key addition, substitution, and linear transformation. On the key addition layer, round subkeys and round input values are exclusive-ored. Substitution layer is made up of n small nonlinear substitutions referred to as S-boxes, and linear transformation layer is a linear transformation in order to diffuse the cryptographic characteristics of substitution layer. A typical example of one round of SPN structures is given in Figure 1.

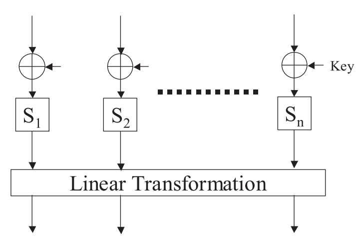

Fig. 1. One round of SPN structures

On r rounds of SPN structures, the linear transformation of the last round, generally, is omitted, because it has no cryptographic significance. Therefore, 2 rounds of SPN structures is given in Figure 2.

S-boxes and linear transformations should be invertible in order to decipher. Therefore we assume that all S-boxes are bijections from Z_2^m to itself. Moreover, throughout this paper, we assume that round subkeys are independent and uniformly distributed.

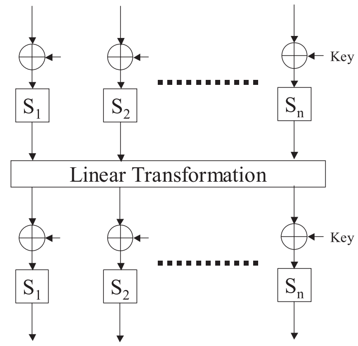

Fig. 2. 2 rounds of SPN structures

Let S be an S-box with m input and output bits. Differential and linear probability of S are defined as the following definition:

Definition 1. *For any given $a, b, \Gamma_a, \Gamma_b \in Z_2^m$, define differential probability $DP^S(a,b)$ and linear probability $LP^S(\Gamma_a, \Gamma_b)$ of S by*

$$DP^S(a,b) = \frac{\#\{x \in Z_2^m | S(x) \oplus S(x \oplus a) = b\}}{2^m}$$

and

$$LP^S(\Gamma_a, \Gamma_b) = \left(\frac{\#\{x \in Z_2^m | \Gamma_a \cdot x = \Gamma_b \cdot S(x)\}}{2^{m-1}} - 1 \right)^2,$$

respectively, where $x \cdot y$ denotes the parity(0 or 1) of bitwise product of x and y.

a and b are called as input and output differences, respectively. Also, Γ_a and Γ_b are called as input and output mask values, respectively.

The strength of an S-box S against differential cryptanalysis is decided by maximum differential probability $\max_{a \neq 0, b} DP^S(a,b)$. The strength of an S-box S against linear cryptanalysis is decided by maximum linear probability $\max_{\Gamma_a, \Gamma_b \neq 0} LP^S(\Gamma_a, \Gamma_b)$.

Definition 2. *The maximum differential probability p and the maximum linear probability q of S are defined by*

$$p = \max_{a \neq 0, b} DP^S(a,b)$$

and

$$q = \max_{\Gamma_a, \Gamma_b \neq 0} LP^S(\Gamma_a, \Gamma_b),$$

respectively.

The maximum differential probability p and the maximum linear probability q for a strong S-box S should be small enough for any input difference $a \neq 0$ and any output mask value $\Gamma_b \neq 0$.

Definition 3. *Differentially active S-box is defined as an S-box given a non-zero input difference and linearly active S-box is defined as an S-box given a nonzero output mask value.*

Since all S-boxes in substitution layer are bijective, if an S-box is differentially/linearly active, then it has a non-zero output difference/input mask value.

For SPN structures, between the differential probability and the number of differentially active S-boxes, there is a relationship which is close. When the number of differentially active S-boxes is many, the differential probability comes to be small, and when the number of differentially active S-boxes is small, the differential probability comes to be big. Therefore, the concept of the branch number was proposed [6]. We call it the branch number from the viewpoint of differential cryptanalysis, the minimum number of differentially active S-boxes of 2 rounds of SPN structures. Also, we call it the branch number from the viewpoint of linear cryptanalysis, the minimum number of linearly active S-boxes of 2 rounds of SPN structures.

The linear transformation $L : (Z_2^m)^n \longrightarrow (Z_2^m)^n$ can be represented by $n \times n$ matrix $M = (m_{ij})$ and $L(x) = Mx$, where $x \in (Z_2^m)^n$ and the addition is bitwise exclusive-ored. For the block cipher E2 [15] and Camellia [1], $m_{ij} \in Z_2$ and the multiplication is trivial. For the block cipher Crypton [12, 13], $m_{ij} \in Z_2^m$ and the multiplication is the bitwise logical-and operation. For the block cipher Rijndael [7], $m_{ij} \in GF(2^m)$ and the multiplication is defined as the multiplication over $GF(2^m)$.

It is easy to show that $L(x) \oplus L(x^*) = L(x \oplus x^*)$ and $DP^L(a, L(a)) = 1$ [5].

Definition 4. *Let L be the linear transformation over $(Z_2^m)^n$. The branch number of L from the view point of differential cryptanalysis, β_d, is defined by*

$$\beta_d = min_{x \neq 0}\{wt(x) + wt(L(x))\},$$

where, $wt(x) = wt(x_1, x_2, \ldots, x_n) = \#\{1 \leq i \leq n | x_i \neq 0\}$.

Throughout this paper, we define $wt(x) = wt(x_1, x_2, \ldots, x_n) = \#\{1 \leq i \leq n | x_i \neq 0\}$ when $x = (x_1, x_2, \ldots, x_n)$. If $x \in Z_2^m$, then $wt(x)$ is the Hamming weight of x.

It is proved that, if $m_{ij} \in Z_2$, then $LP^L(M^t \Gamma_b, \Gamma_b) = 1$. Therefore, we know that $LP^L(\Gamma_a, (M^{-1})^t \Gamma_a) = 1$. Also, if $m_{ij} \in GF(2^m)$, then it is proved that $LP^L(\Gamma_a, C\Gamma_a) = 1$, for some $n \times n$ matrix C over $GF(2^m)$ [9]. Therefore, we can define the branch number β_l from the view point of linear cryptanalysis as follows:

$$\beta_l = \begin{cases} min_{\Gamma_a \neq 0}\{wt(\Gamma_a) + wt((M^{-1})^t \Gamma_a)\}, & \text{if } m_{ij} \in Z_2, 1 \leq i, j \leq n, \\ min_{\Gamma_a \neq 0}\{wt(\Gamma_a) + wt(C\Gamma_a)\}, & \text{if } m_{ij} \in GF(2^m), 1 \leq i, j \leq n. \end{cases}$$

3 Rijndael-like structures

Rijndael is the block cipher composed of SPN structures and its linear transformation consists of ShiftRows transformation and MixColumns transformation.

We analyze some interesting properties of ShiftRows transformation and Mix-columns transformation of Rijndael.

Let $\pi : (Z_2^8)^{16} \longrightarrow (Z_2^8)^{16}$ be the ShiftRows transformation of Rijndael. Let $x = (x_1,x_2,x_3,x_4) = (x_{11},x_{12},x_{13},x_{14}, x_{21}, \ldots, x_{34}, x_{41},x_{42},x_{43},x_{44})$ be the input of π. Figure 3 and 4 illustrate the ShiftRows transformation π of Rijndael.

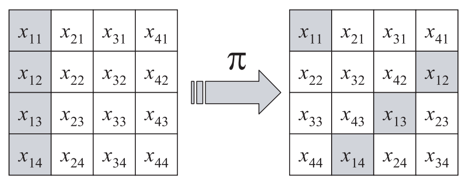

Fig. 3. ShiftRows transformation of Rijndael

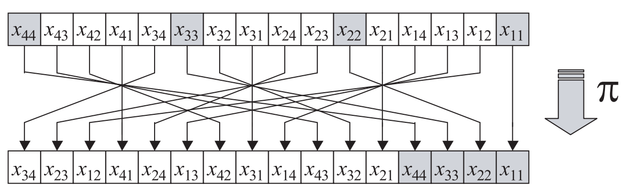

Fig. 4. Another representation of ShiftRows transformation of Rijndael

Let $y = (y_1,y_2,y_3,y_4) = (y_{11},y_{12},y_{13},y_{14}, y_{21}, \ldots, y_{34}, y_{41},y_{42},y_{43},y_{44})$ be the output of π. It is easy to know that, for any $i (i = 1, 2, 3, 4)$, each of bytes of y_i comes from each different x_i. For example, for $y_1 = (y_{11}, y_{12}, y_{13}, y_{14}) = (x_{11}, x_{22}, x_{33}, x_{44})$, x_{11} is a byte coming from x_1. Furthermore, x_{22}, x_{33} and x_{44} are elements of x_2, x_3 and x_4, respectively.

The MixColumns transformation of Rijndael operates on the state column by column, treating each column as a four-term polynomial. Let $\theta = (\theta_1, \theta_2, \theta_3, \theta_4)$ be the MixColumns transformation of Rijndael. Let $y = (y_1, y_2, y_3, y_4) = (y_{11}, y_{12}, y_{13}, y_{14}, y_{21}, \ldots, y_{34}, y_{41},y_{42},y_{43},y_{44})$ be the input of θ and $z = (z_1,z_2,z_3,z_4) = (z_{11},z_{12},z_{13},z_{14}, z_{21}, \ldots, z_{34}, z_{41},z_{42},z_{43},z_{44})$ be the output of θ, respectively. Each of θ_i can be written as a matrix multiplication as follows:

$$\begin{pmatrix} y_{i1} \\ y_{i2} \\ y_{i3} \\ y_{i4} \end{pmatrix} = \begin{pmatrix} 02\ 03\ 01\ 01 \\ 01\ 02\ 03\ 01 \\ 01\ 01\ 02\ 03 \\ 03\ 01\ 01\ 02 \end{pmatrix} \cdot \begin{pmatrix} z_{i1} \\ z_{i2} \\ z_{i3} \\ z_{i4} \end{pmatrix}.$$

In the matrix multiplication, the addition is bitwise exclusive-ored and the multiplication is defined as the multiplication over $GF(2^8)$. Figure 5 illustrates

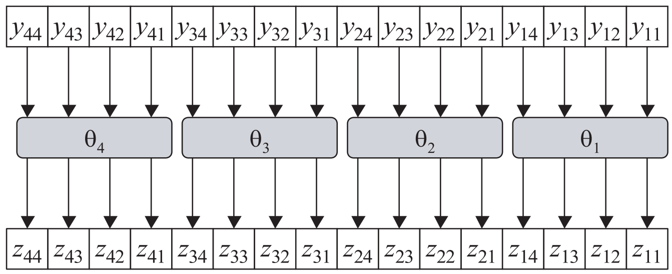

Fig. 5. The MixColumns transformation of Rijndael

the MixColumns transformation θ of Rijndael. We can consider each of θ_i as a linear transformation and we know that the branch number of each of θ_i is 5.

Definition 5. *Rijndael-like structures are the block ciphers composed of SPN structures satisfying the followings:*

(i) *Their linear transformation has the form* $(\theta_1, \theta_2, \theta_3, \theta_4) \circ \pi$.
(ii) *(The condition of* π*) Each of bytes of* y_i *comes from each different* x_i*, where* $x = (x_1, x_2, x_3, x_4)$ *is input of* π *and* $y = (y_1, y_2, y_3, y_4)$ *is output of* π*, respectively.*
(iii) *(The condition of* $\theta = (\theta_1, \theta_2, \theta_3, \theta_4)$*) When we consider each of* θ_i *as a linear transformation, the followings hold:*

$$\beta_d^{\theta_1} = \beta_d^{\theta_2} = \beta_d^{\theta_3} = \beta_d^{\theta_4} \text{ and } \beta_l^{\theta_1} = \beta_l^{\theta_2} = \beta_l^{\theta_3} = \beta_l^{\theta_4}.$$

Rijndael, Square and Crypton are examples of Rijndael-like structures.

Definition 6. *For* $x = (x_1, \ldots, x_n)$*, the pattern of* x*,* γ_x*, is defined by* $\gamma_x = (\gamma_1, \ldots, \gamma_n) \in Z_2^n$*, where, if* $x_i = 0$*, then* $\gamma_i = 0$*, and if* $x_i \neq 0$*, then* $\gamma_i = 1$*.*

If $x = (x_1, x_2, x_3, x_4)$, where $x_1 \neq 0$, $x_2 \neq 0$ and $x_3 = x_4 = 0$, then $\gamma_x = (1, 1, 0, 0)$.

Definition 7. *Let* $x = (x_1, x_2, x_3, x_4)$ *be the input of* π *and* $y = (y_1, y_2, y_3, y_4)$ *be the output of* π*, respectively. For arbitrary* $\gamma \in Z_2^4$ *and* $u = (u_1, u_2, u_3, u_4) \in Z^4$*, We define* $N[\gamma, u]$ *as following:*

$$N[\gamma, u] = \#\{y = \pi(x) | \gamma_x = \gamma, wt(y_i) = u_i, 1 \leq i \leq 4\}.$$

$N[\gamma, u]$ means the number of $y = \pi(x)$ such that $wt(y_i) = u_i (1 \leq i \leq 4)$, when the pattern of input of π is γ. $N[\gamma, u]$ is well-defined and, for any linear transformation which satisfies the condition of π, the values of $N[\gamma, u]$ are all the same for some fixed γ and $u = (u_1, u_2, u_3, u_4)$. The followings are the main properties of $N[\gamma, u]$:

– For some i, if $u_i > wt(\gamma)$, then $N[\gamma, u] = 0$, because $wt(y_i) \leq wt(\gamma_x)$.

– If $u_1 + u_2 + u_3 + u_4 < wt(\gamma)$, then $N[\gamma, u] = 0$, because $\sum_{i=1}^{4} wt(y_i) = \sum_{i=1}^{4} wt(x_i) \geq wt(\gamma_x)$.
– If $\max\{u_1, \ldots, u_4\} = wt(\gamma)$, then $N[\gamma, u] = \binom{wt(\gamma)}{u_1} \cdots \binom{wt(\gamma)}{u_4}$.
– For any permutation ϕ and ρ over $\{1, 2, 3, 4\}$,

$$\begin{aligned} &N[(\gamma_1, \gamma_2, \gamma_3, \gamma_4), (u_1, u_2, u_3, u_4)] \\ &= N[(\gamma_{\phi(1)}, \gamma_{\phi(2)}, \gamma_{\phi(3)} \gamma_{\phi(4)}), (u_{\rho(1)}, u_{\rho(2)}, u_{\rho(3)}, u_{\rho(4)})] \end{aligned}$$

Example 1. For some γ and u, it is easy to determine the value of $N[\gamma, u]$. The followings are the examples:

– $N[(1, 1, 1, 0), (4, 1, 0, 0)] = 0$.
– $N[(1, 1, 1, 0), (1, 1, 0, 0)] = 0$.
– $N[(1, 1, 1, 0), (3, 2, 2, 0)] = 9$.
– $N[(1, 1, 1, 0), (2, 1, 0, 0)] = 3$.

4 The upper bound on the differential and the linear hull probabilities for Rijndael-like structures

To compute the upper bound on the maximum differential probability for $r (r \geq 2)$ rounds of Rijndael-like structures, we assume the following:

$$\beta_d^{\theta_1} = \beta_d^{\theta_2} = \beta_d^{\theta_3} = \beta_d^{\theta_4} = 5 \text{ and } \beta_l^{\theta_1} = \beta_l^{\theta_2} = \beta_l^{\theta_3} = \beta_l^{\theta_4} = 5.$$

and we need the following notations:

– $a = (a_1, \ldots, a_4) = (a_{11}, a_{12}, a_{13}, a_{14}, \ldots, a_{41}, a_{42}, a_{43}, a_{44})$: input difference.
– $b = (b_1, \ldots, b_4) = (b_{11}, b_{12}, b_{13}, b_{14}, \ldots, b_{41}, b_{42}, b_{43}, b_{44})$: output difference.
– $DP_r(a, b)$: differential probability of r rounds whose input difference is a and output difference is b.
– $x^{(i)} = (x_1^{(i)}, \ldots, x_4^{(i)}) = (x_{11}^{(i)}, x_{12}^{(i)}, x_{13}^{(i)}, x_{14}^{(i)}, \ldots, x_{41}^{(i)}, x_{42}^{(i)}, x_{43}^{(i)}, x_{44}^{(i)})$: the input of π at i-th round.
– $y^{(i)} = (y_1^{(i)}, \ldots, y_4^{(i)}) = (y_{11}^{(i)}, y_{12}^{(i)}, y_{13}^{(i)}, y_{14}^{(i)}, \ldots, y_{41}^{(i)}, y_{42}^{(i)}, y_{43}^{(i)}, y_{44}^{(i)})$: the output of π at i-th round, i.e. the input of θ at i-th round.
– $z^{(i)} = (z_1^{(i)}, \ldots, z_4^{(i)}) = (z_{11}^{(i)}, z_{12}^{(i)}, z_{13}^{(i)}, z_{14}^{(i)}, \ldots, z_{41}^{(i)}, z_{42}^{(i)}, z_{43}^{(i)}, z_{44}^{(i)})$: the output of θ at i-th round.

When the branch number is n or $n+1$, it is known that the upper bounds of the maximum differential probability and the linear hull probability for 2 rounds of SPN structures are as follows:

Lemma 1 ([8, 9]).

– *If $\beta_d = n + 1$ or n, then $DP_2(a, b) \leq p^{\beta_d - 1}$.*
– *If $\beta_l = n + 1$ or n, then $LP_2(\Gamma_a, \Gamma_b) \leq q^{\beta_l - 1}$.*

The upper bound on the maximum differential probability for 2 rounds of Rijndael-like structures is obtained by Lemma 1.

Theorem 1.

$$DP_2(a,b) \le \begin{cases} p^{wt(\gamma_{\pi(a)})(\beta_d-1)}, & \text{if } \gamma_{\pi(a)} = \gamma_b, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let $\pi(a) = (a_1^*, a_2^*, a_3^*, a_4^*)$. Then $DP_2(a,b) = \Pi_{i=1}^4 DP_2^{\theta_i}(a_i^*, b_i)$, where, $DP_2^{\theta_i}$ is the differential probability of 2 rounds of SPN structure whose linear transformation is θ_i. By Lemma 1, we know that the upper bound on $DP_2^{\theta_i}(a_i^*, b_i)$ is the followings:

$$DP_2^{\theta_i}(a_i^*, b_i) \le \begin{cases} p^{\beta_d-1}, & \text{if } a_i^* \ne 0,\, b_i \ne 0, \\ 1, & \text{if } a_i^* = 0, b_i = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, the proof is completed.

By Theorem 1, the upper bound on the maximum differential probability for 2 rounds of Rijndael-like structures is p^{β_d-1}. By applying Theorem 1 to Rijndael, we obtain that the maximum differential probability for 2 rounds of Rijndael is bounded by 2^{-24}, because $\beta_d = 5$, $p = 2^{-6}$.

Now, we compute the upper bound on the maximum differential probability for 3 rounds of Rijndael-like structures. To do this, we prove the following:

Lemma 2. *Let $L : (Z_2^m)^n \longrightarrow (Z_2^m)^n$ be the linear transformation whose branch number is β_d. For $\gamma \in Z_2^n$ and $b = (b_1, \ldots, b_n) \in (Z_2^m)^n$ with $wt(\gamma)+wt(b) \ge \beta_d$, we define the set A as following:*

$$A = \{y = (y_1, \ldots, y_n) \in (Z_2^m)^n | \gamma_y = \gamma_b, y = L(x) \text{ for some } x \text{ such that } \gamma_x = \gamma\}.$$

Then, the following holds:

$$\sum_{y\in A} DP_1(y,b) = \sum_{y\in A} DP(y_1,b_1)\cdots DP(y_n,b_n) \le p^{\max\{0,\beta_d - wt(\gamma)-1\}}$$

Proof. Since $\sum_{y\in A} DP_1(y,b) \le \sum_{y\in (Z_2^m)^n} DP_1(y,b) = 1$, it is sufficient to consider the case $\beta_d - wt(\gamma) - 1 > 0$. Without loss of generality, we assume that $wt(b) = k$ and $b_1 \ne 0, \ldots, b_k \ne 0, b_{k+1} = \cdots = b_n = 0$. Then

$$\sum_{y\in A} DP_1(y,b) = \sum_{y\in A} DP(y_1,b_1)\cdots DP(y_k,b_k). \tag{1}$$

We proceed the proof with two cases: $wt(\gamma)+wt(b) = \beta_d$ and $wt(\gamma)+wt(b) > \beta_d$.

(Case 1: $wt(\gamma) + wt(b) = \beta_d$). For any $i(1 \le i \le k)$, let $y_{i,1}, y_{i,2}, \ldots, y_{i,\delta}$ be all possible values of y_i in Equation (1). Then, for each $i(1 \le i \le k)$, $y_{i,1}, y_{i,2}, \ldots, y_{i,\delta}$ are distinct, because L is linear and $wt(\gamma)+wt(b) = \beta_d$. If, for some $i(1 \le i \le k)$, $y_{i,1}, y_{i,2}, \ldots, y_{i,\delta}$ are not distinct, then there exist a pair $(y_{i,l}, y_{i,l'})$ such that $y_{i,l} = y_{i,l'}$, where $y_{i,l}$ is i-th component of $y = L(x)$ and $y_{i,l'}$ is i-th component of $y' = L(x')$, respectively. Since $L(x) \oplus L(x') = L(x \oplus x')$, i-th component of $L(x \oplus x')$ is equal to zero. This is a contradiction of the definition of branch number. Therefore, we can establish the following:

$$\sum_{y \in A} DP_1(y, b) \le p^{k-1} \sum_{y \in A} DP(y_1, b_1) \le p^{k-1} = p^{\beta_d - wt(\gamma) - 1}.$$

(Case 2: $wt(\gamma) + wt(b) > \beta_d$). In this case, $y_{i,1}, y_{i,2}, \ldots, y_{i,\delta}$ are not necessarily distinct, We fix $t = k + wt(\gamma) - \beta_d$ components of nonzero components of y, i.e., $y_1, y_2, \ldots, y_t$. Then, all possible values of each of another components$(y_{t+1}, \ldots, y_k)$ are distinct. Therefore, we can establish the following:

$$\begin{aligned}
&\sum_{y \in A} DP_1(y, b) \\
&\le \sum_{j_1=1}^{2^m-1} DP(j_1, b_1) \cdots \sum_{j_t=1}^{2^m-1} DP(j_t, b_t) \sum_{y \in A, y_i = j_i, 1 \le i \le t} DP(y_{t+1}, b_{t+1}) \cdots DP(y_k, b_k) \\
&\le p^{k-t-1} \sum_{j_1=1}^{2^m-1} DP(j_1, b_1) \cdots \sum_{j_t=1}^{2^m-1} DP(j_t, b_t) \sum_{y \in A, y_i = j_i, 1 \le i \le t} DP(y_{t+1}, b_{t+1}) \\
&\le p^{k-t-1} \sum_{j_1=1}^{2^m-1} DP(j_1, b_1) \cdots \sum_{j_t=1}^{2^m-1} DP(j_t, b_t) \\
&= p^{k-t-1} = p^{\beta_d - wt(\gamma) - 1}.
\end{aligned}$$

Theorem 2. *Let $wt(\gamma_{\pi(a)}) = l$ and $wt(b) = k$. Let $b_{t_1}, \ldots, b_{t_k}$ be the nonzero components of $b = (b_1, b_2, b_3, b_4)$. Then*

$$\begin{aligned}
&DP_3(a, b) \\
&\le p^{l(\beta_d - 1)} \sum_{j_1 = \beta_d - wt(b_{t_1})}^{l} \cdots \sum_{j_k = \beta_d - wt(b_{t_k})}^{l} N[\gamma_{\pi(a)}, (u_1, u_2, u_3, u_4)] \cdot p^{\sum_{i=1}^{k} \max\{0, \beta_d - j_i - 1\}},
\end{aligned}$$

where, each of $u_i (1 \le i \le 4)$ is the following:

$$u_i = \begin{cases} j_s, & \text{if } i = t_s \text{ for some } t_s \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Without loss of generality, we assume that $t_1 = 1, \ldots, t_k = k$. By Theorem 1,

$$\begin{aligned}
DP_3(a,b) &= \sum_{x^{(2)}} DP_2(a,x^{(2)}) DP_1(z^{(2)},b) \\
&= \sum_{\gamma_{x^{(2)}}=\gamma_{\pi(a)}} DP_2(a,x^{(2)}) DP_1(z^{(2)},b) \\
&\le \max_{\gamma_{x^{(2)}}=\gamma_{\pi(a)}} DP_2(a,x^{(2)}) \sum_{z^{(2)}} DP_1(z^{(2)},b) \\
&\le p^{l(\beta_d-1)} \sum_{z^{(2)}} DP_1(z^{(2)},b),
\end{aligned}$$

where, $z^{(2)} = L(x^{(2)}) = (\theta_1(y_1^{(2)}), \theta_2(y_2^{(2)}), \theta_3(y_3^{(2)}), \theta_4(y_4^{(2)}))$. Furthermore, the following three conditions hold:

(i) $\gamma_{z_1^{(2)}} = \gamma_{b_1}, \ldots \gamma_{z_k^{(2)}} = \gamma_{b_k}, \gamma_{z_{k+1}^{(2)}} = \cdots = \gamma_{z_4^{(2)}} = 0$,
(ii) $y_1^{(2)} \neq 0, \ldots, y_k^{(2)} \neq 0, y_{k+1}^{(2)} = \cdots = y_4^{(2)} = 0$,
(iii) $\gamma_{x^{(2)}} = \gamma_{\pi(a)}$.

For each $i (1 \le i \le k)$, since $y_i^{(2)}$ and $z_i^{(2)}$ are the nonzero input and nonzero output of θ_i, respectively, we know that $wt(y_i^{(2)}) + wt(z_i^{(2)}) \ge \beta_d$. Furthermore, since $wt(b_i) = wt(z_i^{(2)})$, we know that $wt(y_i^{(2)}) + wt(b_i) \ge \beta_d$. Therefore, since $wt(y_i^{(2)}) \le wt(\gamma_{x^{(2)}})$, we can establish the following equation:

$$\beta_d - wt(b_i) \le wt(y_i^{(2)}) \le wt(\gamma_{\pi(a)}), 1 \le i \le k.$$

Now, we consider $j_i (1 \le i \le k)$ such that $\beta_d - wt(b_i) \le j_i \le wt(\gamma_{\pi(a)})$. For $(\gamma_1, \ldots, \gamma_4)$ which satisfies that if $1 \le i \le k$, then $wt(\gamma_i) = j_i$ and if $k+1 \le i \le 4$, then $wt(\gamma_i) = 0$, we define the set $A_{(\gamma_1,\ldots,\gamma_4)}$ as following:

$$A_{(\gamma_1,\ldots,\gamma_4)} = \{z^{(2)} = (z_1^{(2)}, \ldots, z_4^{(2)}) | \gamma_{y_i^{(2)}} = \gamma_i, 1 \le i \le 4\}$$

where, $z^{(2)}$ satisfies the three conditions (i), (ii) and (iii).

The set $A_{(\gamma_1,\ldots,\gamma_4)}$ can be empty set, but, the number of non-empty set $A_{(\gamma_1,\ldots,\gamma_4)}$ is $N[\gamma_{\pi(a)}, (j_1, \ldots, j_k, 0, \ldots, 0)]$. If $A_{(\gamma_1,\ldots,\gamma_4)}$ is not empty set, by Lemma 2,

$$\begin{aligned}
\sum_{z^{(2)} \in A_{(\gamma_1,\ldots,\gamma_4)}} DP_1(z^{(2)},b) &= \sum_{z_1^{(2)}} DP_1(z_1^{(2)},b_1) \cdots \sum_{z_k^{(2)}} DP_1(z_k^{(2)},b_k) \\
&\le \Pi_{i=1}^{k} p^{\max\{0,\beta_d-j_i-1\}}.
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\sum_{z^{(2)}} DP_1(z^{(2)},b) \\
&\le \sum_{j_1=\beta_d-wt(b_{t_1})}^{l} \cdots \sum_{j_k=\beta_d-wt(b_{t_k})}^{l} N[\gamma_{\pi(a)}, (u_1,u_2,u_3,u_4)] \cdot p^{\sum_{i=1}^{k} \max\{0,\beta_d-j_i-1\}}.
\end{aligned}$$

Therefore, the proof is completed.

To derive the upper bound on the maximum differential probability for 4 rounds of Rijndael-like structures, we prove the following three lemmas:

Lemma 3. *If* $wt(\gamma_{\pi(a)}) = 2, wt(b) = 3$, *then* $DP_4(a,b) \leq 4p^{19}+6p^{18}+4p^{17}+p^{16}$.

Proof. We assume that $\gamma_b = (1,1,1,0)$. Then we can represent $DP_4(a,b)$ as following:

$$\begin{aligned} DP_4(a,b) &= \sum_{x^{(3)}} DP_3(a,x^{(3)}) DP_1(z^{(3)},b) \\ &= \sum_{i=1}^{4} \sum_{wt(x^{(3)})=i} DP_3(a,x^{(3)}) DP_1(z^{(3)},b) \\ &:= I + II + III + IV. \end{aligned}$$

We know that $wt(y_i^{(2)}) \leq wt(x^{(2)}) = wt(\gamma_{\pi(a)}) = 2$ and $wt(z_i^{(2)}) = wt(x_i^{(3)}) \leq wt(b) = 3$. Since $\beta_d^{\theta_i} = 5$, $wt(x_i^{(3)}) = 3$, where $x_i^{(3)}$ is nonzero component of $x^{(3)}$. Now, we compute the value of I. We can represent I as following:

$$\begin{aligned} I = &\sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a,x^{(3)}) DP_1(z^{(3)},b) + \sum_{\gamma_{x^{(3)}}=(0,1,0,0)} DP_3(a,x^{(3)}) DP_1(z^{(3)},b) \\ &+ \sum_{\gamma_{x^{(3)}}=(0,0,1,0)} DP_3(a,x^{(3)}) DP_1(z^{(3)},b) + \sum_{\gamma_{x^{(3)}}=(0,0,0,1)} DP_3(a,x^{(3)}) DP_1(z^{(3)},b) \\ &:= I_1 + I_2 + I_3 + I_4 \end{aligned}$$

At first, we compute the value of I_1. Since $wt(x_1^{(3)}) = 3$, by Theorem 2,

$$\max_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a,x^{(3)}) \leq p^8 \sum_{j=2}^{2} N[\gamma_{\pi(a)},(j,0,0,0)] p^{4-j} = p^{10}.$$

Since $wt(x_1^{(3)}) = 3$ and $\gamma_b = (1,1,1,0)$, the number of patterns, $(y_1^{(3)}, y_2^{(3)}, y_3^{(3)}, 0)$ is equal to $N[(1,1,1,0),(3,0,0,0)] = 1$. For the pattern $(\gamma_1,\gamma_2,\gamma_3,0)$, by Lemma 2,

$$\begin{aligned} &\sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_1(z^{(3)},b) \\ &= \sum_{\gamma_{y_1^{(3)}}=\gamma_1} DP_1(z_1^{(3)},b_1) \sum_{\gamma_{y_2^{(3)}}=\gamma_2} DP_2(z_2^{(3)},b_2) \sum_{\gamma_{y_3^{(3)}}=\gamma_3} DP_3(z_3^{(3)},b_3) \\ &\leq p^{12-(wt(\gamma_1)+wt(\gamma_2)+wt(\gamma_3))} \leq p^9. \end{aligned}$$

Therefore,

$$I_1 \leq \max_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a,x^{(3)}) \sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_1(z^{(3)},b) \leq p^{19}.$$

By applying the same method, it can be determined that the upper bounds of I_2, I_3 and I_4 are the same with that of I_1. Therefore, we arrive at $I \leq 4p^{19}$. Furthermore, using the same method, we have that $II \leq 6p^{18}$ and $III \leq 4p^{17}$. At last, the upper bound on IV can be computed by Theorem 1 as follows:

$$\begin{aligned}IV &\leq \max_{wt(x^{(3)})=4} DP_3(a, x^{(3)}) \\ &= \max_{wt(x^{(3)})=4} \sum_{x^{(1)}} DP_1(a, x^{(1)}) DP_2(z^{(1)}, x^{(3)}) \\ &\leq \max_{wt(x^{(3)})=4} \max_{z^{(1)}} DP_2(z^{(1)}, x^{(3)}) \leq p^{16}.\end{aligned}$$

Therefore,

$$DP_4(a, b) = I + II + III + IV \leq 4p^{19} + 6p^{18} + 4p^{17} + p^{16}.$$

Lemma 4. *If $wt(\gamma_{\pi(a)}) = 3$, $wt(b) = 2$, then $DP_4(a, b) \leq 4p^{19}+6p^{18}+4p^{17}+p^{16}$.*

Proof. The proof is similar to that of Lemma 3 and is omitted.

Lemma 5. *If $wt(\gamma_{\pi(a)}) = 3$, $wt(b) = 3$, then $DP_4(a, b) \leq 184p^{22} + 912p^{21} + 438p^{20} + 72p^{19} + 4p^{18} + p^{16}$.*

Proof. We assume that $\gamma_b = (1, 1, 1, 0)$. Then we can represent $DP_4(a, b)$ as following:

$$\begin{aligned}DP_4(a, b) &= \sum_{x^{(3)}} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \\ &= \sum_{i=1}^{4} \sum_{wt(x^{(3)})=i} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \\ &:= I + II + III + IV.\end{aligned}$$

We know that $wt(y_i^{(2)}) \leq wt(x^{(2)}) = wt(\gamma_{\pi(a)}) = 3$ and $wt(z_i^{(2)}) = wt(x_i^{(3)}) \leq wt(b) = 3$. Since $\beta_d^{\theta_i} = 5$, $wt(x_i^{(3)}) = 2$ or 3, where $x_i^{(3)}$ is nonzero component of $x^{(3)}$. Now, we compute the value of I. We can represent I as follows:

$$\begin{aligned}I = &\sum_{\gamma_{x^{(3)}}=(1,0,0,0)} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) + \sum_{\gamma_{x^{(3)}}=(0,1,0,0)} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \\ &+ \sum_{\gamma_{x^{(3)}}=(0,0,1,0)} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) + \sum_{\gamma_{x^{(3)}}=(0,0,0,1)} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \\ := &\ I_1 + I_2 + I_3 + I_4.\end{aligned}$$

At first, we compute the value of I_1. Since $\sum_{i=1}^{4} wt(x_i^{(3)}) \geq wt(b) = 3$, if $x_1^{(3)} \neq 0$, then $wt(x_1^{(3)}) = 3$. Therefore, using the same method as in Lemma 3, we know that $I_1 \le p^{22}$ and $I \le 4p^{22}$. Secondly, we compute the value of II. For $\gamma_{x^{(3)}} = (1,1,0,0)$, we have the following:

$$\begin{aligned}
&\sum_{\gamma_{x^{(3)}}=(1,1,0,0)} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \\
&= \sum_{i=2}^{3}\sum_{j=2}^{3} \sum_{wt(x_1^{(3)})=i, wt(x_2^{(3)})=j} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b)
\end{aligned}$$

Since $wt(x_1^{(3)}) = 2, wt(x_2^{(3)}) = 2$, by Theorem 2,

$$\begin{aligned}
\max_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_3(a, x^{(3)}) &\le p^{12} \sum_{j_1=3}^{3}\sum_{j_2=3}^{3} N[\gamma_{\pi(a)}, (j_1, j_2, 0, 0)] p^{8-j_1-j_2} \\
&= p^{12} \cdot N[(1,1,1,0), (3,3,0,0)] p^2 \\
&= p^{14}.
\end{aligned}$$

Since $wt(x_1^{(3)}) = 2, wt(x_2^{(3)}) = 2$ and $\gamma_b = (1,1,0,0)$, the number of pattern whose form is $(z_1^{(3)}, z_2^{(3)}, z_3^{(3)}, 0)$ is equal to $N[(1,1,1,0),(2,2,0,0)] = 6$. For each of $(\gamma_1, \gamma_2, \gamma_3, 0)$, by Lemma 2,

$$\begin{aligned}
&\sum_{\gamma_{y_i^{(3)}}=\gamma_i, 1\le i\le 3} DP_1(z^{(3)}, b) \\
&= \sum_{\gamma_{y_1^{(3)}}=\gamma_1} DP_1(z_1^{(3)}, b_1) \sum_{\gamma_{y_2^{(3)}}=\gamma_1} DP_1(z_2^{(3)}, b_2) \sum_{\gamma_{y_3^{(3)}}=\gamma_1} DP_1(z_3^{(3)}, b_3) \\
&\le p^{12-(wt(\gamma_1)+wt(\gamma_2)+wt(\gamma_3))} = p^8.
\end{aligned}$$

Therefore, $\sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_1(z^{(3)}, b) \le 6p^8$ and we arrive at the following:

$$\begin{aligned}
&\sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \\
&\le \max_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_3(a, x^{(3)}) \sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=2} DP_1(z^{(3)}, b) \\
&\le 6p^{22}.
\end{aligned}$$

Using the same method, we can have the followings:

$$\sum_{wt(x_1^{(3)})=2, wt(x_2^{(3)})=3} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \le 3(3p^{15} + p^{14})p^7,$$

$$\sum_{wt(x_1^{(3)})=3, wt(x_2^{(3)})=2} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \le 3(3p^{15} + p^{14})p^7,$$

$$\sum_{wt(x_1^{(3)})=3, wt(x_2^{(3)})=3} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \leq (6p^{16} + 6p^{15} + p^{14})p^6.$$

Therefore, we arrive at

$$\sum_{\gamma_{x^{(3)}}=(1,1,0,0)} DP_3(a, x^{(3)}) DP_1(z^{(3)}, b) \leq 6p^{22} + 6(3p^{15} + p^{14})p^7 + (6p^{16} + 6p^{15} + p^{14})p^6$$

and

$$II \leq 6[6p^{22} + 6(3p^{15} + p^{14})p^7 + (6p^{16} + 6p^{15} + p^{14})p^6],$$

because the upper bound on summation for distinct $\gamma_{x^{(3)}}$ such that $wt(\gamma_{x^{(3)}}) = 2$ is the same as the upper bound on summation for $\gamma_{x^{(3)}} = (1, 1, 0, 0)$. Using the same method, we have the following:

$$III \leq 4[24p^{21} + 27(3p^{16} + p^{15})p^5 + 9(9p^{17} + 6p^{16} + p^{15})p^4 + (24p^{18} + 27p^{17} + 9p^{16} + p^{15})p^3].$$

At last, the upper bound on IV can be computed by Theorem 1 as following:

$$IV \leq \max_{wt(x^{(3)})=4} DP_3(a, x^{(3)}) \leq \max_{wt(x^{(3)})=4, z^{(1)}} DP_2(z^{(1)}, x^{(3)}) \leq p^{16}.$$

Therefore, we arrive at

$$DP_4(a, b) = I + II + III + IV \leq 184p^{22} + 912p^{21} + 438p^{20} + 72p^{19} + 4p^{18} + p^{16}.$$

Therefore, the proof is completed.

Theorem 3 shows the upper bound on the maximal differential probability for 4 rounds of Rijndael-like structures and this is the main result of this paper.

Theorem 3.

$$DP_4(a, b) \leq \max\{4p^{19} + 6p^{18} + 4p^{17} + p^{16}, 184p^{22} + 912p^{21} + 438p^{20} + 72p^{19} + 4p^{18} + p^{16}\}.$$

Proof. We compute the upper bound on $DP_4(a, b)$ for the value of $wt(\gamma_{\pi(a)})$ and $wt(b)$. Since $\beta_d = 5$, if $wt(\gamma_{\pi(a)}) + wt(b) \leq 4$, then $DP_4(a, b) = 0$. Therefore, it is sufficient to compute the upper bound on $DP_4(a, b)$, when $wt(\gamma_{\pi(a)}) + wt(b) \geq 5$.

(i) If $wt(\gamma_{\pi(a)}) = 4$, then, by Theorem 1,

$$DP_4(a, b) = \sum_{x^{(2)}} DP_2(a, x^{(2)}) DP_2(z^{(2)}, b) \leq \max_{x^{(2)}} DP_2(a, x^{(2)}) \leq p^{16}.$$

(ii) If $wt(b) = 4$, then, by Theorem 1,

$$DP_4(a, b) = \sum_{x^{(2)}} DP_2(a, x^{(2)}) DP_2(z^{(2)}, b) \leq \max_{x^{(2)}} DP_2(a, x^{(2)}) \leq p^{16}.$$

(iii) If $wt(\gamma_{\pi(a)}) = 2, wt(b) = 3$, then, by Lemma 3,

$$DP_4(a, b) \leq 4p^{19} + 6p^{18} + 4p^{17} + p^{16}.$$

(iv) If $wt(\gamma_{\pi(a)}) = 3, wt(b) = 2$, then, by Lemma 4,

$$DP_4(a, b) \leq 4p^{19} + 6p^{18} + 4p^{17} + p^{16}.$$

(v) If $wt(\gamma_{\pi(a)}) = 3, wt(b) = 3$, then, by Lemma 5,

$$DP_4(a, b) \leq 184p^{22} + 912p^{21} + 438p^{20} + 72p^{19} + 4p^{18} + p^{16}.$$

When $p \leq 2^{-3}$, the maximum differential probability for 4 rounds of Rijndael-like structures is bounded by $4p^{19} + 6p^{18} + 4p^{17} + p^{16}$.

Using the similar method as in Theorem 3, we can compute the upper bound on the linear hull probability for 4 rounds of Rijndael-like structures.

Theorem 4.

$$LP_4(a, b) \leq \max\{4q^{19}+6q^{18}+4q^{17}+q^{16}, 184q^{22}+912q^{21}+438q^{20}+72q^{19}+4q^{18}+q^{16}\}.$$

We know that the differential probabilities for 5 rounds of Rijndael-like structures are smaller than or equal to the maximum differential probability for 4 rounds of Rijndael-like structures.

$$DP_5(a, b) = \sum_{x^{(4)}} DP_4(a, x^{(4)}) DP_1(z^{(4)}, b) \leq \max_{x^{(4)}} DP_4(a, x^{(4)}).$$

Similarly, we know that the differential probabilities for $r(r \geq 5)$ rounds of Rijndael-like structures are smaller than or equal to the maximum differential probability for 4 rounds of Rijndael-like structures. Therefore, the upper bound on the maximum differential probability and the linear hull probability for 4 rounds of Rijndael-like structures in Theorem 3 and Theorem 4 is the upper bound for $r(r \geq 5)$ rounds of Rijndael-like structures.

By applying our method to Rijndael, since $p = q = 2^{-6}$ and $\beta_d = \beta_l = 5$, the upper bound on $DP_4(a, b)$ and $LP_4(a, b)$ is the following:

$$4 \times 2^{-114} + 6 \times 2^{-108} + 4 \times 2^{-102} + 2^{-96} \approx 1.06 \times 2^{-96}.$$

5 Conclusion

In this paper, we have proposed a new method for upper bounding the maximum differential probability and the maximum linear hull probability for Rijndael-like structures. We have proved that the maximum differential probability for 4 rounds of Rijndael-like structures is bounded by $4p^{19} + 6p^{18} + 4p^{17} + p^{16}$, when the maximum differential probability for S-boxes is $p(\leq 2^{-3})$. Also, we have proved that the maximum linear hull probability for 4 rounds of Rijndael-like structures is bounded by $4q^{19} + 6q^{18} + 4q^{17} + q^{16}$, when the maximum linear hull probability for S-boxes is $q(\leq 2^{-3})$. By applying our method to Rijndael, an improved upper bound 1.06×2^{-96} is obtained.

References

1. Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block ciher suitable for multiple platforms - design and analysis. In Douglas R. Stinson and Stafford Tavares, editors, *Selected Areas in Cryptography*, volume 2012 of *Lecture Notes in Computer Science*, pages 39–56. Springer, 2000.
2. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystem. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - Crypto'90*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer-Verlag, Berlin, 1991.
3. Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.
4. C.E.Shannon. Communication Theory of Secrecy System. *Bell System Technical Journal*, 28:656–715, October 1949.
5. Joan Daemen, René Govaerts, and Joos Vandwalle. Correlation matrices. In Bart Preneel, editor, *Fast Software Encryption, Second International Workshop*, volume 1008 of *Lecture Notes in Computer Science*, pages 275–285. Springer, 1994.
6. Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher square. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.
7. Joan Daemen and Vincent Rijmen. Rijndael, AES Proposal. *http://www.nist.gov/aes*, 1998.
8. Seokhie Hong, Sangjin Lee, Jongin Lim, Jaechul Sung, Donghyeon Cheon, and Inho Cho. Provable security against differential and linear cryptanalysis for the spn structure. In Bruce Schneier, editor, *Fast Soft Encryption, 7th International Workshop*, pages 273–283, 2000.
9. Ju-Sung Kang, Seokhie Hong, Sangjin Lee, Okyeon Yi, Choonsik Park, and Jongin Lim. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks. *ETRI Journal*, 23(4):158–167, 2001.
10. Liam Keliher, Henk Meijer, and Stafford Tavares. Improving the upper bound on the maximum average linear hull probability for rijndael. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography, 8th Annual International Workshop*, volume 2259 of *Lecture Notes in Computer Science*, pages 112–128. Springer, 2001.
11. Liam Keliher, Henk Meijer, and Stafford Tavares. New method for upper bounding the maximum average linear hull probability for spns. In Birgit Pfitzmann, editor, *Advances in Cryptology - Eurocrypt 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 420–436. Springer-Verlag, Berlin, 2001.
12. Chae Hoon Lim. CRYPTON, AES Proposal. *http://www.nist.gov/aes*, 1998.
13. Chae Hoon Lim. A revised version of crypton - crypton v1.0 -. In Lars Knudsen, editor, *Fast Software Encryption, 6th International Workshop*, volume 1636 of *Lecture Notes in Computer Science*, pages 31–45. Springer, 1999.
14. Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology - Eurocrypt'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, 1994.
15. NTT-Nippon Telegraph and Telephone Corporation. E2: Efficient Encryption algorithm, AES Proposal. *http://www.nist.gov/aes*, 1998.