Security Assessment of Hierocrypt and Rijndael against the Differential and Linear Cryptanalysis (Extended Abstract)

Kenji Ohkuma*, Hideo Shimizu*, Fumihiko Sano†, Shinichi Kawamura*

* Toshiba Corporate R & D Center, †Toshiba SI Thechnology Center

Abstract. The authors analyze the security of Hierocrypt-3(128-bit) and Hierocrypt-L1(64-bit) designed on the nested SPN(NSPN) structure against the differential and linear cryptanalysis, and found that they are sufficiently secure, e.g., the maximum average differential and linear hull probabilities (MACP and MALHP) are bounded by 2^{-96} for 4-round of Hierocrypt-3; those probabilities are bounded by 2^{-48} for 4-round of Hierocrypt-L1. The authors get these results by extending the provable security theorem by Hong et al.. Furthermore, the extended theory is applied to Rijndael, and found that MACP and MALHP of 4-round Rijndael are bounded by 2^{-96}. This outperforms the best previous result by Keliher et al..

1 Introduction

We estimate the security of two block ciphers, Hierocrypt-3 and Hierocrypt-L1, against the differential cryptanalysis(DC) and linear cryptanalysis(LC).

Hierocrypt-3 and Hierocrypt-L1 consists of the Nested SPN (NSPN) structure, which is a hierarchical structure, where an S-box in a higher-level consists of the lower-level SPN structure [8, 2]. An advantage of the NSPN structure is that main security properties such as the maximum differential characteristic probability (MDCP) and the maximum linear characteristic probability (MLCP) can be evaluated hierarchically.

Recently, Hong et al. proved the theorem of the provable security against LC and DC, that the maximum average linear hull probability (MALHP) and the maximum average differential probability (MADP) are bounded, when the linear transformation module is the maximum distance separable(MDS) [5].

In this paper, we show that the theorem of provable security can be hierarchically applicable to the nested SPN structure where any linear module in any level MDS. This new result has been applied to Hierocrypt-3 and Hierocrypt-L1, and it is found that the upper bound of maximum average differential/linear probabilities for 2-round Hierocrypt-3 is no more than 2^{-96}, and those for 2-round Hierocrypt-L1 is no more than 2^{-48}.

The result is also applied to Rijndael(AES) which can be equivalently transformed into a nested SPN form. Then, we found that the upper bound of differential/linear probabilities for 4 rounds are bounded by 2^{-96}. The result outperforms the best known result 2^{-75} for T rounds($7 \leq T10$) by Keliher et al.[6].

The construction of this paper is as follows. In the next section, several kinds of security measures against DC and LC are defined, and fundamental security properties on SPN cipher are presented. In Section 3, the security properties of Hierocrypt-3 and Hierocrypt-L1 against DC and LC are shown, by using an extension of provable theory by Hong et al.. In Section 4, the new provable theorem is applied to Rijndael.

2 Preliminary

2.1 Security against Differential and Linear Cryptanalysis

The differential and linear cryptanalysis are effective against general symmetric block cryptosystems, the former of which was proposed by Biham and Shamir [1] and the latter proposed by Matsui [7]. The number of plaintext-ciphertext pairs needed for the cryptanalysis is known to be the same order of the inverse of the maximum differential/linear probability of data randomizing part removing 2 or 3 rounds of both ends. Therefore, in the component design, the maximum differential and linear probabilities (MDP and MLP) are the most important security measures for block ciphers. That is, the cipher is safer against these attacks, when both probabilities are sufficiently small.

In general, the cipher consists of an iteration of round functions which depend on respective round keys. The dependency on keys makes it difficult to estimate the values for MDP and MLP. Therefore two classes of approximation for these probabilities are used. The first class consists of MDCP and MLCP where the summation of intermediate states is replaced into one intermediate state with the maximum probability. The second class consists of MADP and MALHP where key-averaged values are used but the summation of intermediated states are done. The second ones are considered to be better estimation measures. When the intermediate rounds have a sufficiently small MADP and MALHP, the cipher is called to have a provable security (in the meaning of key average). In the following subsection, the definition of these probabilities are given.

2.2 Differential and Linear Probabilities

Definition 1. *For an n-bit function f, the differential probability DP^f and the linear probability LP^f are defined as follows.*

$$DP^f(\Delta x \to \Delta y) \equiv \frac{\#\{x|f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n}, \quad (1)$$

$$LP^f(\Gamma y \to \Gamma x) \equiv \left|2 \cdot \frac{\#\{x|x \cdot \Gamma x = f(x) \cdot \Gamma y\}}{2^n} - 1\right|^2, \quad (2)$$

where Δx, Δy are input and output differences; Γx and Γy are input and output masks.

The main part of most block ciphers is multiple-round structure. Let T-round structure as follows.

$$E_T = \rho[k_T] \circ \rho[k_{T-1}] \circ \cdots \circ \rho[k_1] .$$

$$x_i = \rho[k_i](x_{i-1}) , \qquad i = 1, \ldots, T.$$

For E_T, the input(plaintext) is $x = x_0$, and the output(ciphertext) is $y = x_T$.

The maximum differential probability for a T-round encryption E_T is defined as

Definition 2 (MDP/MLP). *Let x, y and k be an input, an output and a key vectors. Then, the maximum differential probability(MDP) and the maximum linear probability(MLP) for a T-round encryption E_T is defined as follows.*

$$MDP(E_T) \equiv \max_{\Delta x \neq 0, \Delta y, k} \sum_{\Delta x_1, \Delta x_2, \ldots, \Delta x_{T-1}} \prod_{i=1}^{T} DP^{\rho_i[k_i]}(\Delta x_{i-1} \to \Delta x_i) \quad (3)$$

$$MLP(E_T) \equiv \max_{\Gamma x, \Gamma y \neq 0, k} \sum_{\Gamma x_1, \Gamma x_2, \ldots, \Gamma x_{T-1}} \prod_{i=1}^{T} LP^{\rho_i[k_i]}(\Gamma x_i \to \Gamma x_{i-1}) \quad (4)$$

If MDP/MLP is sufficiently small, it can be assured that there is no weak key against DC/LC.

The estimation of MDP and MLP is very difficult for most practical block ciphers. Therefore, instead of MDP and MLP, key-averaged values MADP and MALHP are used as the second best security measures.

Definition 3 (MADP/MALHP). *The maximum average differential probability(MADP) and the maximum average linear hull probability(MALHP)* *are defined as follows.*

$$MADP(E_T) \equiv \max_{\Delta x \neq 0, \Delta y} \operatorname*{ave}_{k} \sum_{\Delta x_1, \ldots, \Delta x_{T-1}} \prod_{i=1}^{T} DP^{\rho_i[k_i]}(\Delta x_{i-1} \rightarrow \Delta x_i) \quad (5)$$

$$MALHP(E_T) \equiv \max_{\Gamma x, \Gamma y \neq 0} \operatorname*{ave}_{k} \sum_{\Gamma x_1, \ldots, \Gamma x_{T-1}} \prod_{i=1}^{T} LP^{\rho_i[k_i]}(\Gamma x_i \rightarrow \Gamma x_{i-1}) \quad (6)$$

A block cipher is called provably secure against DC and LC, if the upper bounds of MADP and MALHP can be estimated theoretically.

For most practical ciphers, even MADP and MALHP are difficult to estimate, because the summation for intermediate states should be done. The next best approximation is a single path approximation MDCP/MLCP, where the summation for intermediate states is substituted into the maximum value for intermediate states.

Definition 4 (MDCP/MLCP). *The maximum differential characteristic probability(MDCP) and the maximum linear characteristic probability(MLCP) are defined as follows.*

$$MDCP(E_T) \equiv \max_{\Delta x \neq 0, \Delta y} \operatorname*{ave}_{k} \sum_{\Delta x_1, \ldots, \Delta x_{T-1}} \prod_{i=1}^{T} DP^{\rho_i[k_i]}(\Delta x_{i-1} \rightarrow \Delta x_i) \quad (7)$$

$$MLCP(E_T) \equiv \max_{\Gamma x, \Gamma y \neq 0} \operatorname*{ave}_{k} \sum_{\Gamma x_1, \ldots, \Gamma x_{T-1}} \prod_{i=1}^{T} LP^{\rho_i[k_i]}(\Gamma x_i \rightarrow \Gamma x_{i-1}) \quad (8)$$

2.3 SPN structure

The fundamental structure of SPN cipher is an iteration of the round function, which consists of key addition, word-wise substitution (S-box layer) and block-size mixing (diffusion layer) [9, 3, 4]. In the rest of this paper we omit to draw key addition for simplicity. Besides the fundamental part, some modification is applied such as the key addition just before the output.

In the SPN cipher, the diffusion layer provides an avalanche effect. An important measure of avalanche effect is the minimum number of active S-boxes both for differential and linear, where an active S-box is defined as follows.

Definition 5 (Active S-box). *A differential active S-box is defined as an S-box with non-zero input difference. A linear active S-box is defined as an S-box with non-zero output mask.*

The following lemma gives the upper bounds for MDCP and MLCP by using the lower bounds of active S-boxes and the differential/linear probability of S-box.

Lemma 1. *Let p be the maximum differential probability of S-box, and let q be the maximum linear probability of S-box. When the lower bounds for differential/linear active S-boxes are $\mathcal{LAS}_{\mathrm{D}}$ and $\mathcal{LAS}_{\mathrm{L}}$, respectively. Then the characteristic probabilities MDCP and MLCP are bounded as follows.*

$$MDCP(E_T) \leq p^{\mathcal{LAS}_{\mathrm{D}}} \ , \quad MLCP(E_T) \leq q^{\mathcal{LAS}_{\mathrm{L}}} \ . \tag{9}$$

In the analysis of active S-box number, the branch number of diffusion layer has an important role. Consider the SPS structure shown Fig. 5, where two S-box layers containing M-parallel S-boxes are connected by the diffusion layer. The branch number is defined for differential and linear cryptanalysis as follows.

Definition 6 (Branch Number). *The differential branch number $\mathcal{B}_{\mathrm{D}}$ is defined as the minimum number of active S-boxes in the SPS structure for a non-zero input difference. The linear branch number $\mathcal{B}_{\mathrm{L}}$ is defined as the minimum number of active S-boxes in the SPS structure for a non-zero output mask.*

The branch numbers are bounded by the following lemma.

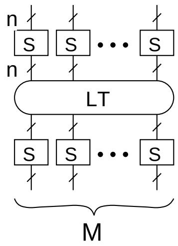

Fig. 1. Simple SPS Structure

Lemma 2. *Both differential and linear branch numbers are bounded by $M+1$, where the diffusion layer consists of M-parallel S-boxes.*

$$\mathcal{B}_{\mathrm{D}} \leq M+1 \ , \quad \mathcal{B}_{\mathrm{L}} \leq M+1 \ . \tag{10}$$

When both branch numbers take their maximum values, the diffusion layer is called **MDS**, as such diffusion layer can be made based on the maximum distance separable code.

For the multiple-round SPN structure, the upper bound of maximum differential/linear characteristic probability (MDCP/MLCP) is easily estimated.

Lemma 3. *When the maximum differential/linear probability of S-box is p/q, and the differential/linear branch number is $\mathcal{B}_{\mathrm{D}}/\mathcal{B}_{\mathrm{L}}$ for T-round SPN encryption E_T, its MDCP and MLCP are bounded as follows.*
For even T

$$MDCP(E_T) \leq p^{\mathcal{B}_{\mathrm{D}} T/2} \ , \quad MDCP(E_T) \leq p^{\mathcal{B}_{\mathrm{L}} T/2} \ . \tag{11}$$

For odd T

$$MDCP(E_T) \leq p^{\mathcal{B}_{\mathrm{D}}(T-1)/2+1} \ , \quad MDCP(E_T) \leq p^{\mathcal{B}_{\mathrm{L}}(T-1)/2+1} \ . \tag{12}$$

Hong et al. proved the following important theorem for the provability of SPN cipher.

Theorem 1 (Hong et al.). *If the diffusion layer is MDS, i.e., $\mathcal{B}_{\mathrm{D}} = \mathcal{B}_{\mathrm{L}} = M+1$, and $T \geq 2$,*

$$MACP(E_T) \leq p^M \ , \quad MALHP(E_T) \leq q^M \ . \tag{13}$$

If the invertible diffusion layer satisfies $\mathcal{B}_{\mathrm{D}} = \mathcal{B}_{\mathrm{L}} = M$, and $T \geq 2$,

$$MACP(E_T) \leq p^{M-1} \ , \quad MALHP(E_T) \leq q^{M-1} \ . \tag{14}$$

3 Nested SPN Structure and Hierocrypt

3.1 Nested SPN structure (NSPN)

The nested SPN is a hierarchical SPN structure, where an S-box in a higher level consists of SPN in the lower level. Figs. 2 shows a fundamental concept of the nested SPN structure. We propose the following conditions to achieve an efficient data randomization [8].

(a) The final round of SPN consists only of an S-box layer (not followed by a diffusion layer) in all levels;
(b) All permutations are MDS in each level;
(c) The number of rounds is even in all levels except for the highest;
(d) Bit-wise key additions are located directly before all lowest-level S-box layers and directly after the final.

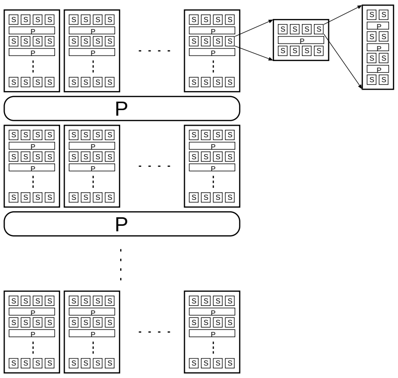

Fig. 2. Nested SPN structure

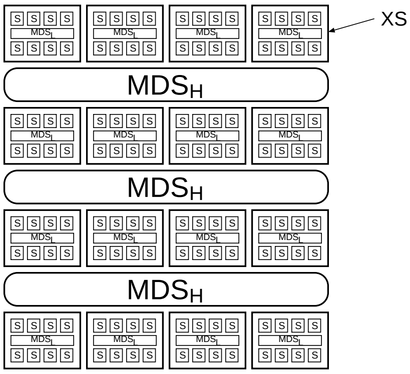

Fig. 3. 4-Round Nested SPN Cipher

3.2 Hierocrypt

The Hierocrypt is a family of NSPN block ciphers which satisfy the conditions from (a) through (d) in the previous subsection. The newest versions are Hierocrypt-3 and Hierocrypt-L1 [1]. Hierocrypt-3 is a 128-bit block cipher which supports 3 kinds of key length: 128-, 192- and 256-bit. Hierocrypt-L1 is a 64-bit block cipher which supports a 128-bit key. Fig.4 shows data randomizing parts of both algorithms.

For both algorithms, all lower-level S-boxes s (8-bit) are the same, and the maximum differential/linear probabilities are 2^{-6}. The lower-level diffusion mds_{L}(32-bit) is the same for both algorithms. The mds_{L} satisfies the MDS condition, i.e., the branch number is 5. The higher-level diffusion layer MDS_{H} of Hierocrypt-3 is of 128-bit, and the branch number is 5. The higher-level diffusion layer MDS_{H} of Hierocrypt-L1 is of 64-bit, and the branch number is 3.

4 Security of Hierocrypt against Differential/Linear Cryptanalysis

The upper bounds for 4 security measures MDCP, MLCP, MADP and MALHP are estimated in this section for Hierocrypt-3 and Hierocrypt-L1.

4.1 Upper bounds for MDCP and MLCP

Before analyzing Hierocrypt, we consider a general case of two-level NSPN cipher where the round numbers in both levels are two, the higher-level

[1] The oldest versions are 128-bit ciphers, Hierocrypt Type-I and Type-II [8]

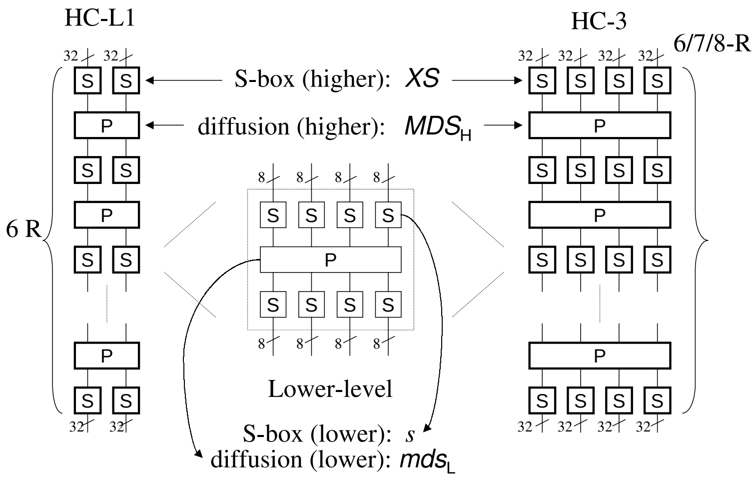

Fig. 4. Structure of Hierocrypt

S-box layer consists of M_1 parallel XS, and the lower-level S-box layer consists of M_2 parallel s (See Fig.5). Similarly for the simple SPN case, the fundamental unit of security estimation is 2-round structure also for NSPN cipher.

For a pair of inputs with non-zero difference, at least $M_1 + 1$ higher-level S-boxes (XS's) are active, and each active XS contains no less than $M_2 + 1$ active (lower-level) S-boxes (s's). Therefore, we get the following two lemmas.

Lemma 4. *In Fig.5, the number of differential/linear active(lower-level) S-boxes is no less than* $(M_1 + 1)(M_2 + 1)$.

Lemma 5. *If the maximum differential/linear probability for the lower S-box* s *is* p/q*, the MDCP and the MLCP satisfy the following inequalities.*

$$MDCP \leq p^{(M_1+1)(M_2+1)} \ , \quad MLCP \leq q^{(M_1+1)(M_2+1)} \ . \qquad (15)$$

The fundamental probabilities and branch numbers are given for Hierocrypt as follows.

Hierocrypt-3:

$$p = q = 2^{-6} \ , \quad M_1 = M_2 = 4. \qquad (16)$$

Hierocrypt-L1:

$$p = q = 2^{-6} \ , \quad M_1 = 2, \ M_2 = 4. \qquad (17)$$

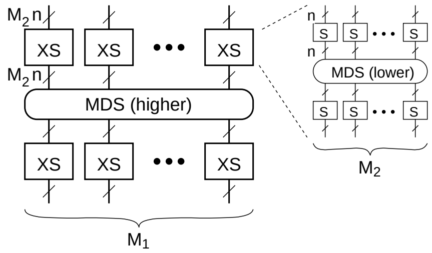

Fig. 5. 2-level Nested SPS module(NSPS)

For Hierocrypt-3, from Eqs. (15) and (16), the upper bound of MDCP/MLCP for 2-round Hierocrypt-3 is estimated as $2^{-6\times(4+1)\times(4+1)} = 2^{-150}$. The upper bound for 1-round Hierocrypt-3 is estimated by assuming only one XS is active, i.e., $2^{-6\times(4+1)} = 2^{-30}$. Combining these results, we can estimate MDCP/MLCP of Hierocrypt-3 for more rounds(Fig.6).

For Hierocrypt-L1, from Eqs. (15) and (17), the upper bound of MDCP/MLCP for 2-round is estimated as $2^{-6\times(4+1)\times(2+1)} = 2^{-90}$. The upper bound for 1-round is the same to that of Hierocrypt-3, i.e., $2^{-6\times(4+1)} = 2^{-30}$. Combining these results, we can estimate MDCP/MLCP of Hierocrypt-L1 for more rounds(Fig.6).

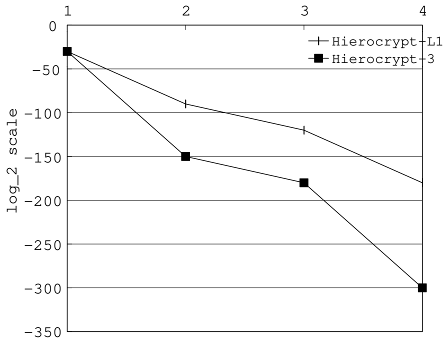

Fig. 6. Upper bound of MDCP/MLCP

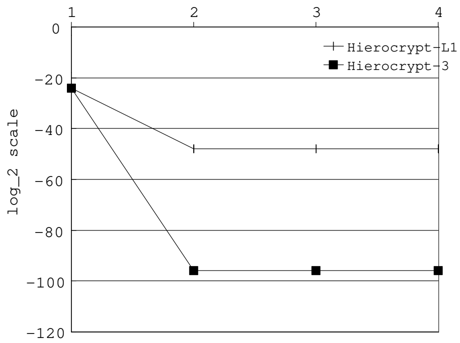

Fig. 7. Upper bound of MADP/MALHP

4.2 Provable Security of Hierocrypt(MADP and MALHP)

Before analyzing Hierocrypt, we consider a general case of Fig.5. The MADP and MALHP [2] for the nested SPS structure(NSPS, Fig.5) is estimated by the following Theorem 2.

Theorem 2. *If the key is uniformly random, and if the maximum differential/linear probability of lower-level S-box is p/q, MADP and MALHP of NSPS is bounded as follows,*

$$MADP(NSPS) \leq p^{M_1 M_2} \ , \tag{18}$$
$$MALHP(NSPS) \leq q^{M_1 M_2} \ . \tag{19}$$

Proof. Theorem 1 assures that the MADP of XS is bounded by p^{M_2}. Then we can consider XS as a function whose maximum differential probability is no more than p^{M_2} in the meaning of key average. Again, Theorem 1 assures that the MADP of 2-level nested SPN (NSPS) is bounded by

$$MADP(NSPS) \leq \left(p^{M_2}\right)^{M_1} = p^{M_1 M_2}.$$

Quite similarly, we can prove the inequality for the linear probability MALHP. ¶

Now, we can estimate the MADP and MALHP of Hierocrypt.

Hierocrypt-3 Substituting the fundamental quantities in Eq.16 to Theorem 2 (Eqs. (18) and (19)), we get the upper bounds of MADP and MALHP for 2-round as follows.

$$MADP(NSPS) \leq \left(2^{-6}\right)^{4\times 4} = 2^{-96} \ , \tag{20}$$
$$MALHP(NSPS) \leq \left(2^{-6}\right)^{4\times 4} = 2^{-96} \ . \tag{21}$$

Hierocrypt-L1 Substituting the fundamental quantities in Eq.17 to Theorem 2 (Eqs. (18) and (19)), we get the upper bounds of MADP and MALHP for 2-round as follows.

$$MADP(NSPS) \leq \left(2^{-6}\right)^{4\times 2} = 2^{-48} \ , \tag{22}$$
$$MALHP(NSPS) \leq \left(2^{-6}\right)^{4\times 2} = 2^{-48} \ . \tag{23}$$

[2] The maximum probabilities in the meaning of key average.

5 Provable Security of Rijndael

Rijndael is the most famous SPN-type cipher, and recently adopted as FIPS encryption algorithm, Advanced Encryption Standard(AES). The linear transformation consists of a byte shift operations and a mix column operation. The mix column operation is MDS module for a 1-byte (8-bit) word, that is, no less than 5 from 8 bytes on input and output are active for non-zero input differential.

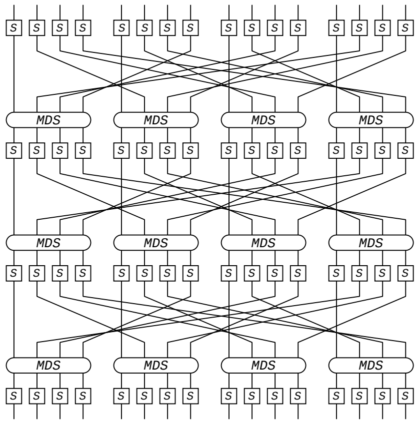

Fig. 8. 4-R Rijndael

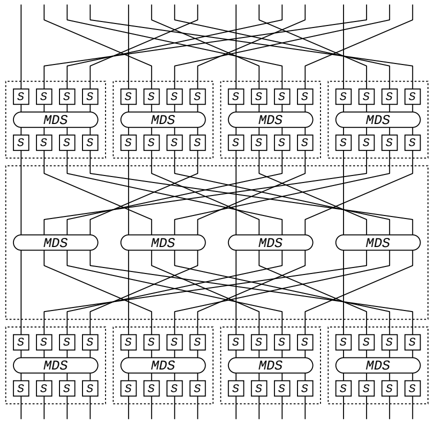

Fig. 9. nested SPN expression of Rijndael

Two major results are known for the security of Rijndael against the differential/linear cryptanalysis. The first result, given by the designers, is that both MDCP and MLCP are no more than 2^{-150}, which is derived from the fact that consecutive 4 rounds contain no less than 25 active S-boxes and that the maximum differential/linear probability is 2^{-6}. The second result is given by Keliher et al. for the upper bound of MALHP for several rounds from 2 through 10 [6]. With an large-scale calculation, they get the upper bounds 2^{-75} for $7 \leq T \leq 10$ (Fig.10).

5.1 Equivalent Transformation to NSPN

Rijndael can be equivalently transformed into a nested SPN form with $M_1 = M_2 = 4$ (Figs.8 and 9. The property of mix column module have already shown that the lower-level linear transform is MDS. Fig. 9 can be

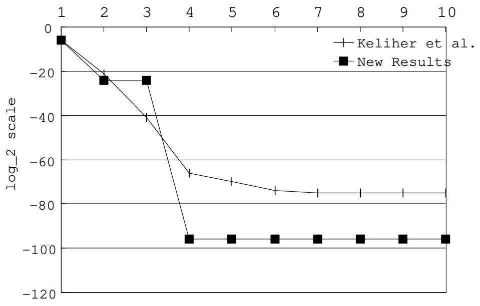

Fig. 10. New upper bound of MDCP/MLCP for Rijndael

shown that the higher-level linear transform is also MDS for 32-bit word as follows. If input difference is not zero, at least 1 from 4 mix column modules is active. And each input and output bytes are connected to respective 32-bit XS-boxes. Therefore, the higher-level linear transform, the large dotted rectangle in the center of Fig. 9, is MDS for 32-bit words. Quite similarly, we can show that the higher-level linear transform is MDS for LC. Therefore, we found the new and best bound of MADP and MALHP for Rijndael; 2^{-96} for 4 and more even rounds, and 2^{-24} for 2 rounds. Using these results, we can estimate MACP and MALHP of Rijndael for an arbitrary round number(Fig.10).

Furthermore, it is easily seen that 4 consecutive rounds of Rijndael contains at least 25 active S-boxes.

6 Conclusion

Hierocrypt is a block cipher family designed on the nested SPN (NSPN) structure. We have discussed the security of nested SPN structure against the differential and linear cryptanalysis, and succeeded in estimating the upper bounds of characteristic probabilities, MDCP and MLCP for the newest versions Hierocrypt-3(128-bit) and Hierocrypt-L1(64-bit). For 4-round Hierocrypt-3, both MDCP and MLCP is found to be no more than 2^{-150}. For 4-round Hierocrypt-L1, both MDCP and MLCP is found to be no more than 2^{-90}.

Furthermore, we extend the provable security theory for SPN by Hong et al. to NSPN structure. Based on the theorem, we found that both MACP and MALHP are bounded by 2^{-96} for 2-round Hierocrypt-3, and that both MACP and MALHP are bounded by 2^{-48} for 2-round Hierocrypt-L1.

These results assure that Hierocrypt-3 and Hierocrypt-L1 are very secure against the differential/linear cryptanalysis, as the proposed minimum round numbers 6 for both algorithms is sufficiently large compared to 2.

Furthermore, we found that MACP and MALHP for 4-round Rijndael is no more than 2^{-96}. In the derivation of this result, we use the fact that Rijndael is equivalently transformed into the nested SPN form. This upper bound largely outperforms the result 2^{-75} for T-round Rijndael $(7 \leq T \leq 10)$ by Keliher et al..

References

1. E. Biham and A. Shamir. Differential cryptanalysis of des-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.
2. Toshiba Corporation Corporate R & D Center. *Block cipher family Hierocrypt*, 2000. https://www.toshiba.co.jp/rdc/contact/index.htm.
3. J. Daemen, L.R. Knudsen, and V. Rijmen. The block cipher square. *Fast Software Encryption, LNCS*, 1267:149–165, 1997.
4. J. Daemen, L.R. Knudsen, and V. Rijmen. *AES Proposal: Rijndael*, 2000. http://www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip.
5. S. Hong, S. Lee, J. Lim, J. Sung, and D. Cheon. "provable security against differential and linear cryptanalysis for the spn structure". In *Fast Software Encryption 2000*, LNCS 1636. Springer-Verlag, 2000.
6. L. Keliher, H. Meijer, and S. Tavares. New method for upper bounding the maximum average linear hull probability for spns. In *Eurocrypt 2001*, volume 2045 of *LNCS*, pages 420–436, 2001.
7. M. Matsui. Linear cryptanalysis method for des cipher. In *Eurocrypt'93*, volume 765 of *LNCS*, pages 386–397. Springer Verlag, 1994.
8. K. Ohkuma, H. Muratani, F. Sano, and S. Kawamura. The block cipher hierocrypt. In *Selected Areas in Cryptography, SAC 2000*, LNCS 2012, pages 72–88, 2000.
9. V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. DeWin. The cipher shark. *Fast Software Encryption, LNCS*, 1039:99–112, 1996.