Security Analysis of HyRal

Heung Youl YOUM, Jung Hwan Song, Sun Young Lee

February 4, 2011

Executive Summary

This report presents the security analysis results of the block cipher, so-called HyRal. The evaluation is based on theoretical derivations. We have not found flaws or weaknesses in the design, which could lead to cryptanalytic attacks with respect to the state-of-the-art.

The HyRal is an iterated cipher, which has 128bits block length and supports key length of 128-bits, 192-bits and 256-bits. It is relatively easy to be convinced about the resistance of HyRal with respect to differential and linear cryptanalysis.

It is further believed that any practical attacks against HyRal are not possible with respect to the state-of-the-art. That is, we conclude that HyRal might be resistant to some well-known analysis such as differential attack, higher order differential attack, linear attack(including Truncated Linear Attack), interpolation attacks, algebraic attack (including XL attack and XSL attack), related key attack, and the existence of weak keys and semi-weak keys.

Lastly, we mention that a concentrated, longer analysis might reveal properties that we did not detect in the limited-time review.

Index

1. Overview

- Techniques to be Evaluated : HyRAL 128-bit Block Cipher

- Types of security analysis for HyRAL the evaluation team has studied

  - ・Differential Attack (including Truncated Differential Attack, Impossible Differential Attack),
  - ・Higher Order Differential Attack,
  - ・Linear Attack (including Truncated Linear Attack),
  - ・Interpolation Attack,
  - ・Algebraic Attack (including XL attack and XSL attack),
  - ・Related Key Attacks and the existence of weak keys and semi-weak keys
  - ・(Optional) Any other attacks specific to HyRAL and Heuristic security

- References for evaluation

  - ・A set of documents and data submitted to CRYPTREC ((http://www.cryptrec.go.jp/english/topics/cryptrec_20101001_callforattack.html).

- Period of cooperation and time span of reports submission.

  - ・October 1, 2010 - January 31, 2011

- Evaluation team
  - ・Heung Youl YOUM, Coordination and Team leader, Professor/SCH university, Korea
  - ・Jung Hwan Song, Differential analysis, Professor/Hanyang University, Korea
  - ・Sun Young Lee, Linear analysis, Professor/SCH university, Korea
  - ・Anonymous Independent Researcher, other analysis

2. Structural features and characteristics

This report is to evaluate a cryptographic algorithm, HyRAL, which has 128-bits block length and supports key length of 128, 192 and 256bits. In other word, HyRAL can accommodate specs equivalent to AES. It has a 4-way generalized Feistel Structure of 24 rounds for 128bits key length, and 32 rounds for 192, 256-bits key length. The rounds are consists of G1, G2, F1, F2 functions which have 4-round Feistel structure to make the cryptanalysis hard.

This cryptographic algorithm has some new features, which are newly designed 4x4 MDS transformation, having non circulant matrix, 4 different types of expanded functions G1, G2, F1, F2. There are many block ciphers using 4x4 MDS transformation, but most of them use circulant matrix. But HyRAL has 4x4 MDS non-circulant matrix. Because using circulant matrix, special case is inevitable. The case of 4bytes same code input to MDS result 4bytes same code. Therefore difference between input too output are all same. HyRAL is Feistel Type block cipher, which decrypt sequence is same as encrypt sequence using only SubKey sequence as inverse. But HyRAL is different with other Feistel Type block chpher.

2.1 Design philosophy

RyRAL was developed to achieve sufficient robustness against known decoding technologies. It was also designed so that its coding technology can be expanded for use in the following three applications:

- Achieve both coding and authorization based on a calculation using one key and one block coding.
- Use of hash functions based on block coding technology.
- Multi-block coding

2.2 Structural outline of HyRAL

2.2.1 Overalll Structure of HyRAL

In overall structure of HyRAL, key length of 128, 192 to 256 bits exist. It is of a generalized FEISTEL structure consisting of 4 data lines, connecting the 4 different algorithm functions of G1, G2, F1, and F2. HyRAL is different from ordinal Feistel Type which has same process of both encryption and decryption by only changing SubKeys sequence. In decryption, HyRAL uses inverse expanded functions respectably. SubKey sequence is also change.

2.2.2 Basic Function (fi function)

fi (i=1, 2, 3, 4, 5, 6, 7, 8)

Its input is 32 bits and output is 32 bits. Depending on transposition of input bytes, there are 8 basic functions.

There are S layer and P layer following transposition of input bytes. In the S layer, use 8-bit [S-box] having the maximum linear/differential probability of 2^{-6}, in 4 parallel data line. The P Layer shall have an MDS matrix of 4-byte input/output.(Figure 1)

In addition, perform transposition immediately before input to the function. As there are 8 ways of transposition, denote them as T1 – T1 by transposition type.

Thus, fi function corresponding to the transposition of T1 is f1, fi function corresponding to the transposition of T2 is f2, and there are 8 types of fi functions, f1-f8

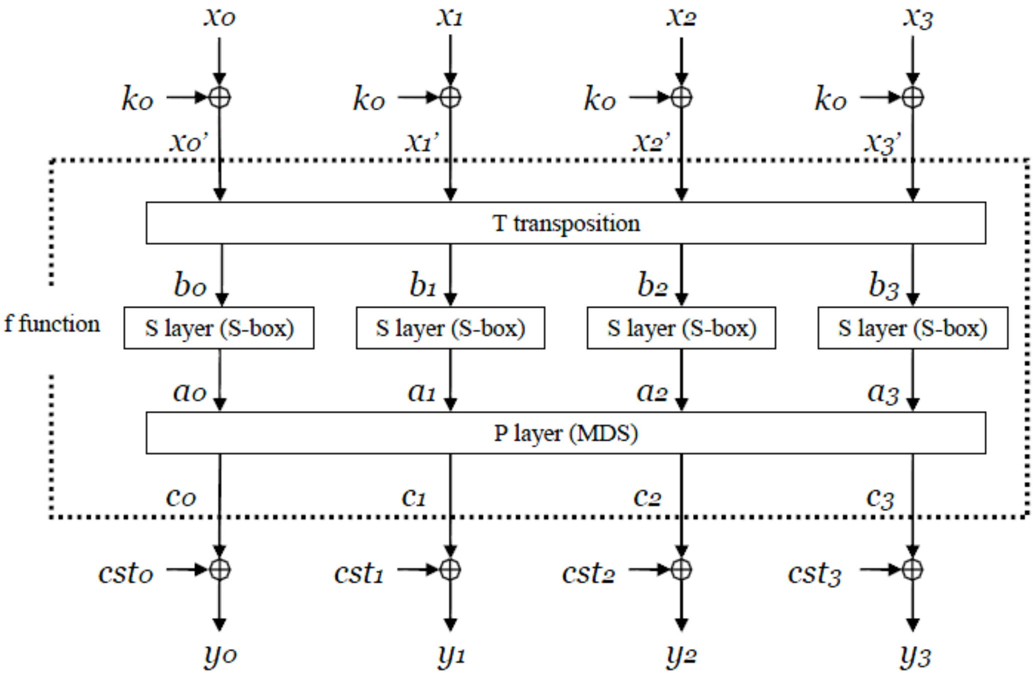


Figure 1 - fi function

Here, k0, k1, k2, k3 are 8-bit element of fi function input key IKi. IKi = (k0, k1, k2, k3) cst0, cst1, cst2, cst3 are constants 0x11, 0x22, 0x44, 0x88, and for clearing any singular point (All Null).

2.2.3 Expanded Function

G1, G2, F1, F2

The functions have 128-bit input size and 128-bit output size, using the basic function (fi function). Four types of extension functions are available : G1, G2, F1, F2 G function uses fi function once in each round. Figure 2 and Figure 3 show G1 function and G2 function.

F function uses fi function twice in each round. Figure 4 and Figure 5 show F1 function and F2 function.

In decrypt, calculate an inverse function with the lower end of the cipher algorithm as input, and use fi function which is same as the cipher.

An intermediate key is inputted in F function, and IKi,0, IKi,1, IKi,2, IKi,3 are 32-bit elements of IKi.

* IKi= ([MSW] IKi,0, IKi,1, IKi,2, IKi,3 [LSW])

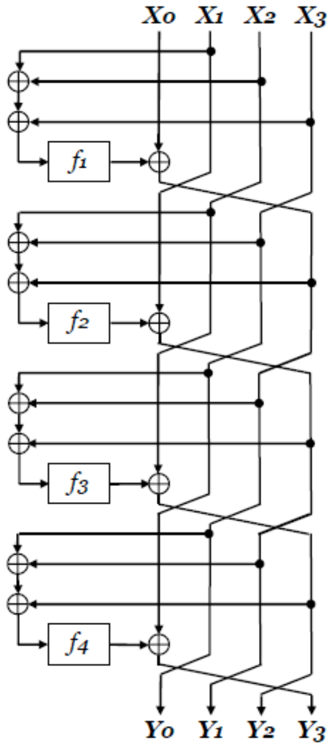


Figure 2 - G1 Function(Cipher)

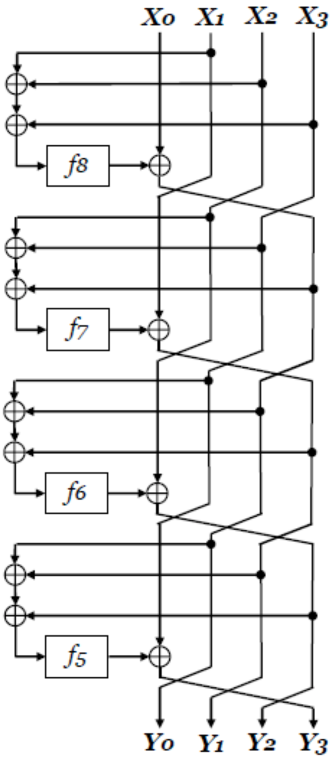


Figure 3 - G2 Function(Cipher)

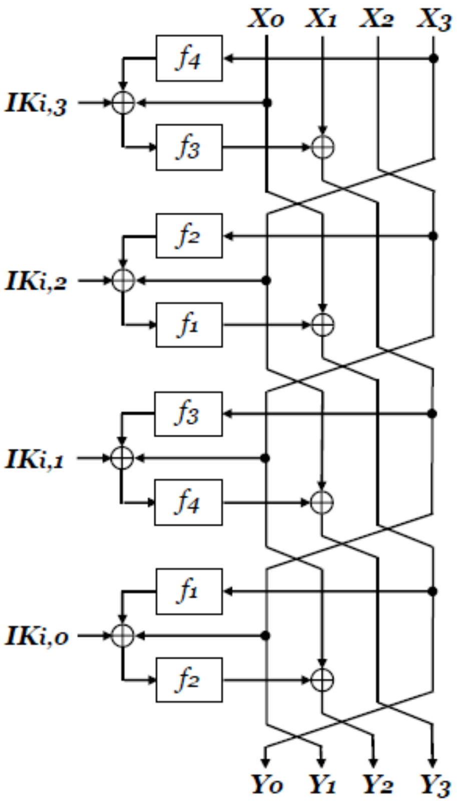


Figure 4 - F1 Function(Cipher)

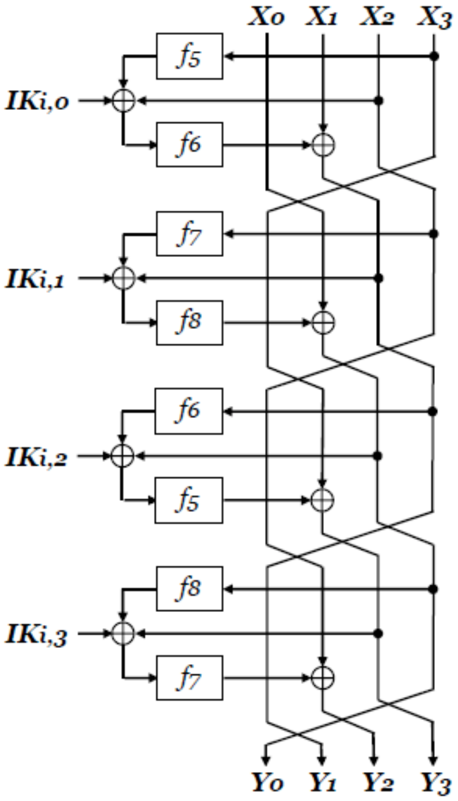


Figure 5 - F2 Function(Cipher)

2.2.4 Key Generator

Using G1 and G2 functions, create the intermediate key KMi (Key material) from the secret key OK. Then, based on it, generate the extension keys (RKi and IKi) to be used in each round of encryption conversion. Use different key processing modes when size of the secret key is 128 bits and when it is 192 bits and 256 bits. The former is referred to as Single Key Mode, while the other Double Key Mode.

In the case of Double Key Mode, process the secret key OK by dividing it into OK1 and OK2.

2.2.5 Overall Structure of HyRAL

Figure 6 shows ciphers when the key size of HyRAL is 128 bits and Figure 7 shows ciphers when the key sizes are 192 and 256 bits.

For the key size of 128 bits, use 7 types of round keys RK1 to RK7. And 4 types of fi function input keys IK1 to IK4.

For the key size of 192 and 256 bits, use 9 types of round keys RK1 to RK9. And 6 types of fi function input keys IK1 to IK6.

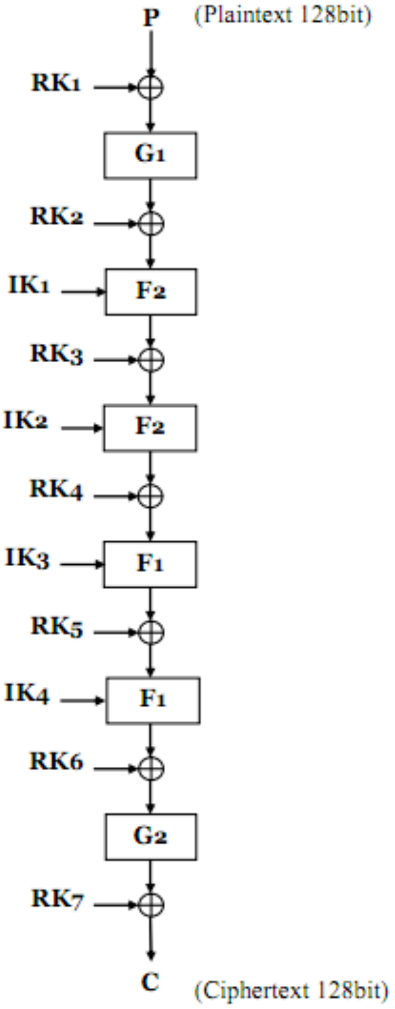


Figure 6 - Key 128bit(Cipher)

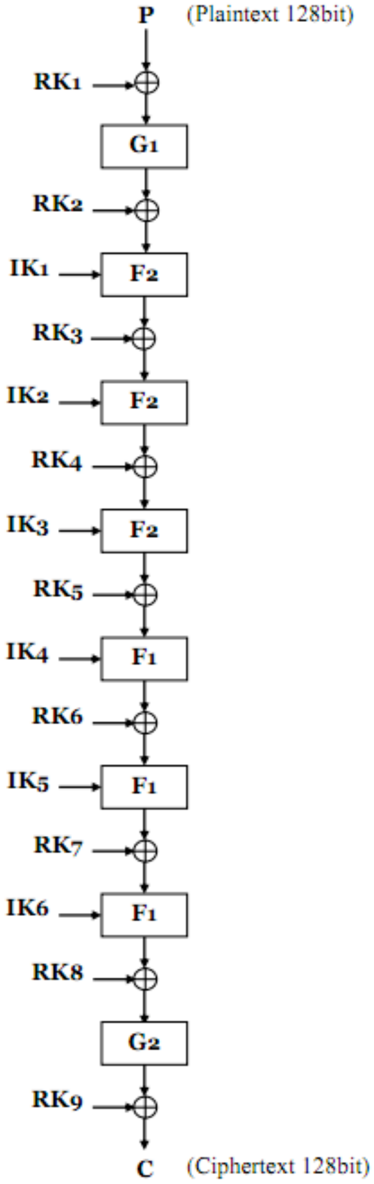


Figure 7 - Key 192bit, 256bit(Cipher)

2.2.6 Generation of S-BOX

S-BOX is comprised of a combination of the inverse function s =z-1 (However, z-1=0) on GF(2^8), which is a nonlinear layer, affine transformation Expression 1, which is a linear function, and a gray code transformation Expression 2

Figure 8 shows the generation process. The maximum linear and maximum differential probability of S-BOX is 2^-6

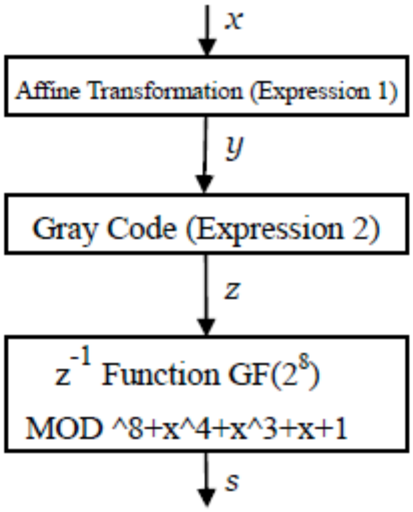


Figure 8 - Generation of S-BOX

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

$$\begin{pmatrix} z_7 \\ z_6 \\ z_5 \\ z_4 \\ z_3 \\ z_2 \\ z_1 \\ z_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix}$$

Expression1 : Affine Transformation y=(x+64)MOD256 Expression2 : Gray Code z=y□(y≫1)

3. Security analysis result of Hyral

3.1 Differential cryptanalysis

The resistance of a block cipher to classical differential cryptanalysis is estimated by analyzing the maximum probability of differential trails. In the case of HyRAL, one can easily find a bound on these probabilities by considering the branch number of the diffusion layer (MDS in the case of HyRAL) and the maximum differential probabilities of the S-boxes (2^{-6}).

We suppose that:

- Round Function is a swap function in large function assuming;
  - One Fundamental function is included one round function of G1 and G2; and
  - Two Fundamental functions are included one Round function of F1 and F2,

based on

- 128-bit secret key for 24 Rounds;
- 192-bit and 256-bit secret key for 32 Rounds;
- Maximum differential probability of the S-boxes is 2^{-6} ;
- Minimum branch Number of the MDS is 5.

We use that each byte is represented to a single bit as follows:

- 0 : a byte without difference
- 1 : a byte with a difference.

The maximal difference propagation probability of the S-box in HyRAL is 2^{-6}. Since the block sizes are 128, we can allow no more than 21 active S-boxes(128/6=21.3) in the characteristics for HyRAL. We consider the difference propagation of the MDS as described in Figure 9.

(a_0, a_1, a_2, a_3)	→	(c_0,c_1,c_2,c_3)
(0,0,0,0)	$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 3 & 3 & 2 & 1 \\ 1 & 2 & 2 & 2 \\ 7 & 3 & 1 & 2 \\ 7 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$	(0,0,0,0)
(0,0,0,1)		(1,1,1,1)
(0,0,1,0)		(1,1,1,1)
(0,0,1,1)		(1,0,1,1)
(0,1,0,0)		(1,1,1,1)
(0,1,0,1)		(1,0,1,1)

(0,1,1,0)		(1,0,1,1)
(0,1,1,1)		(1,1,1,1)
(1,0,0,0)		(1,1,1,1)
(1,0,0,1)		(1,1,1,1)
(1,0,1,0)		(1,1,1,1)
(1,0,1,1)		(1,1,1,1)
(1,1,0,0)		(0,1,1,1)
(1,1,0,1)		(1,1,1,1)
(1,1,1,0)		(1,1,1,1)
(1,1,1,1)		(1,1,1,1)

Figure 9- Difference propagation of the MDS

In HyRAL, we have found nine differentials characteristics on 11 rounds with 19 active S-boxes, 11 rounds with 20 active S-boxes, and 11 rounds with 21 active S-boxes. In HyRAL, there is no 12 rounds differential characteristic. Table 1 shows the number of Active S-box for round 11 and 12 on particular difference of plaintext.

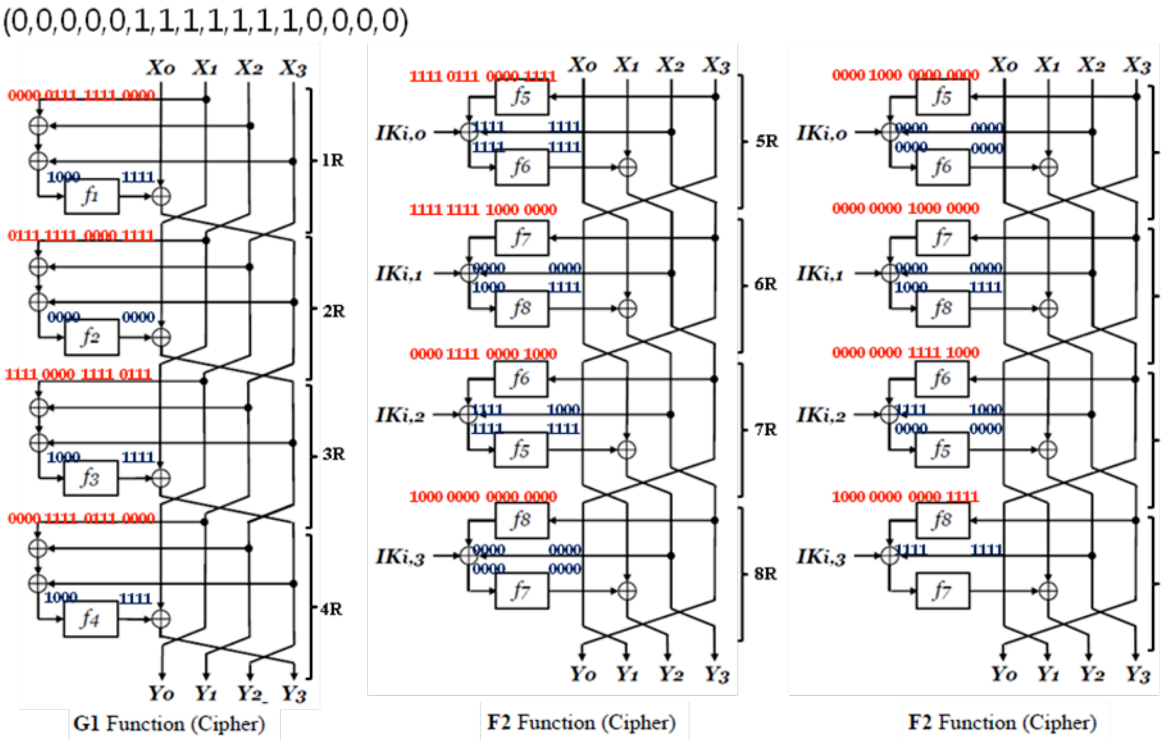
Table 1 – Number of Active S-box for round 11 and 12 on particular difference of plaintext

	Difference of Plaintext	Round	Number of Active S-boxes	Round	Number of Active S-boxes
1	(0,0,0,0,0,1,1,1,1,1,1,1,0,0,0,0)	11	19	12	23
2	(0,0,0,0,1,0,1,1,1,1,1,1,0,0,0,0)	11	19	12	23
3	(0,0,0,0,1,1,0,1,1,1,1,1,0,0,0,0)	11	19	12	23
4	(0,0,0,0,1,1,1,0,1,1,1,1,0,0,0,0)	11	19	12	23
5	(0,1,0,0,1,0,0,1,1,1,1,1,1,1,1,1)	11	20	12	23
6	(1,0,0,0,0,1,1,0,1,0,0,1,1,0,1,1)	11	20	12	23
7	(1,1,0,0,0,0,1,0,1,1,1,1,1,0,1,1)	11	21	12	24
8	(1,1,1,1,0,0,0,0,0,0,1,1,0,1,1,1)	11	20	12	24
9	(1,1,1,1,0,0,0,0,0,0,1,1,1,0,1,1)	11	20	12	24

An upper bound of probabilities on differential characteristic for 12-rounds is $(2^{-6})^{23} = 2^{-138}$ or $(2^{-6})^{24} = 2^{-144}$. Therefore, there are no effective differential characteristics for HyRAL in 12 or more rounds.

An upper bound of probabilities on differential characteristic for 11-rounds is $(2^{-6})^{19} = 2^{-114}$, $(2^{-6})^{20} = 2^{-120}$ or $(2^{-6})^{21} = 2^{-126}$ which is greater than 2^{-128}. Even if an attacker tries to attack with the above 11-round differential on HyRAL, we expect that 24 rounds(128-bit secret key) or 32 rounds(192-bit and 256-bit secret key) are enough to resist against differential cryptanalysis.

Notice that the same values in the nonzero differences from output bytes of f_i functions are assumed. Considering other differential propagations not in Figure 10, it is expecting that those differential propagations imply significantly low probabilities and do not contribute an effective differential cryptanalysis of full-round HyRAL.

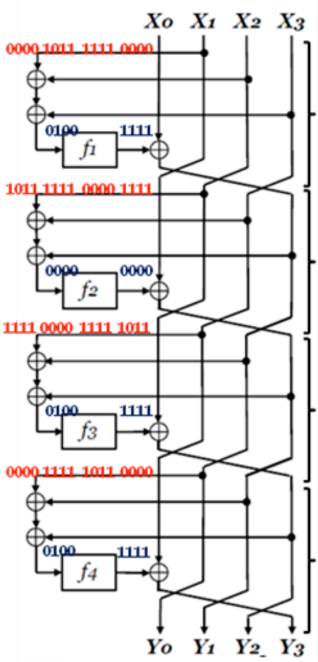


G1 Function (Cipher)

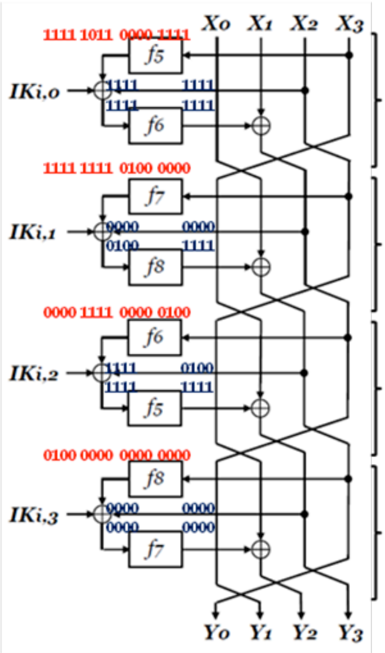
F2 Function (Cipher)

F2 Function (Cipher)

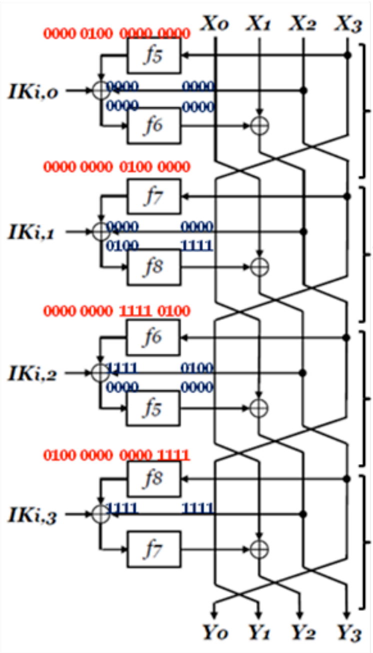
(0,0,0,0,1,0,1,1,1,1,1,1,0,0,0,0)



G1 Function (Cipher)

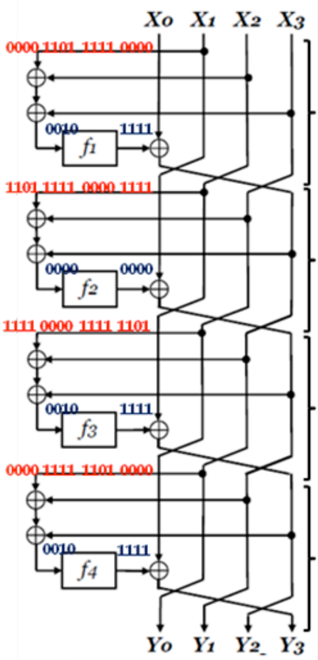


F2 Function (Cipher)

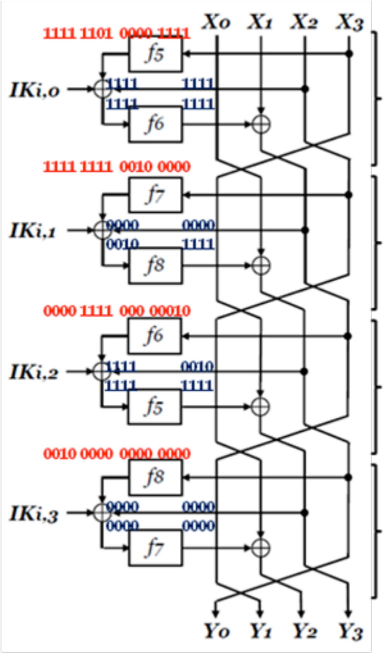


F2 Function (Cipher)

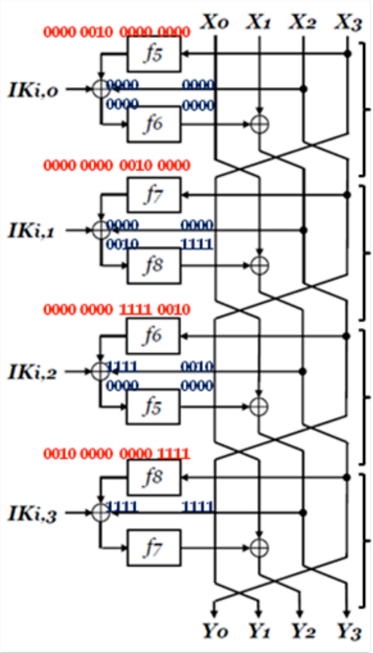
(0,0,0,0,1,1,0,1,1,1,1,1,0,0,0,0)



G1 Function (Cipher)

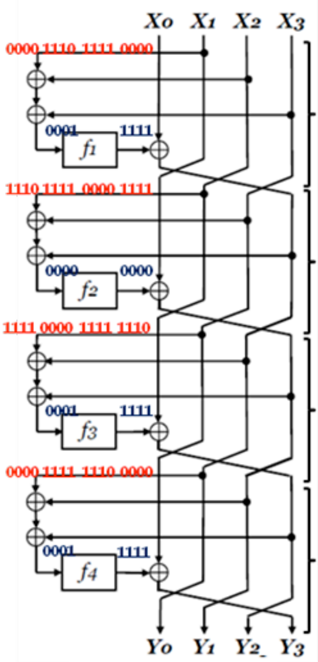


F2 Function (Cipher)

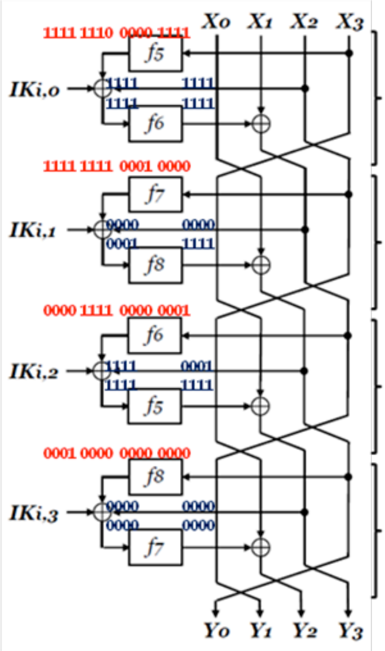


F2 Function (Cipher)

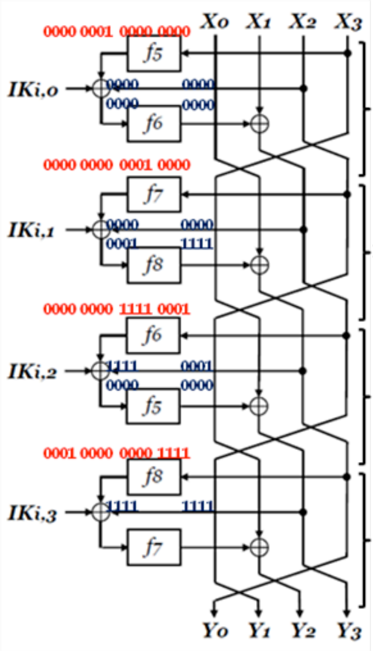
(0,0,0,0,1,1,1,0,1,1,1,1,0,0,0,0)



G1 Function (Cipher)

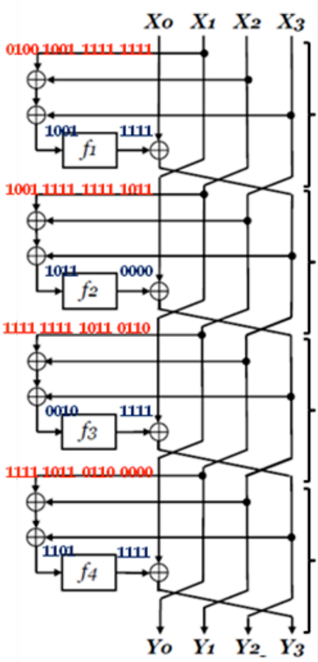


F2 Function (Cipher)

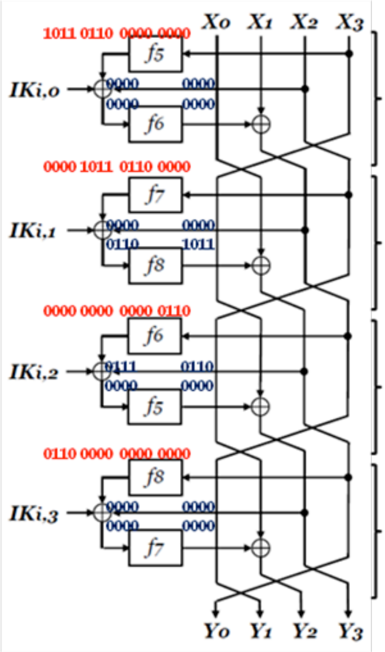


F2 Function (Cipher)

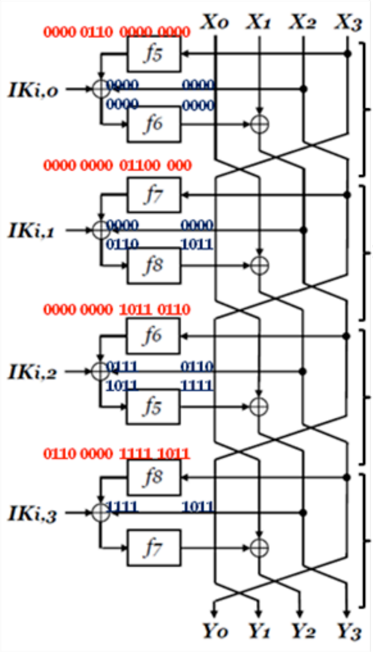
(0,1,0,0,1,0,0,1,1,1,1,1,1,1,1,1)



G1 Function (Cipher)

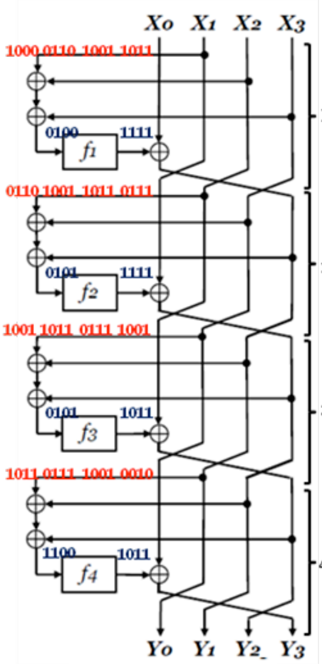


F2 Function (Cipher)

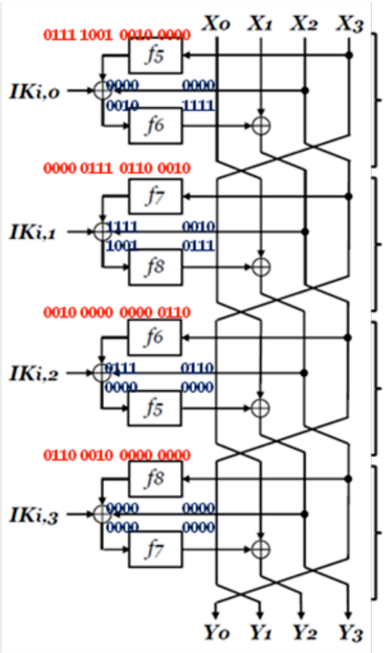


F2 Function (Cipher)

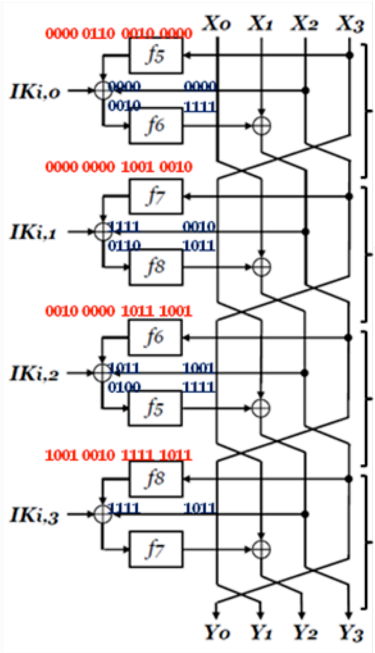
(1,0,0,0,0,1,1,0,1,0,0,1,1,0,1,1)



G1 Function (Cipher)

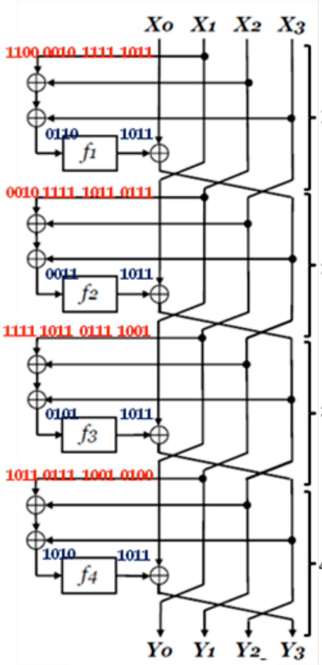


F2 Function (Cipher)

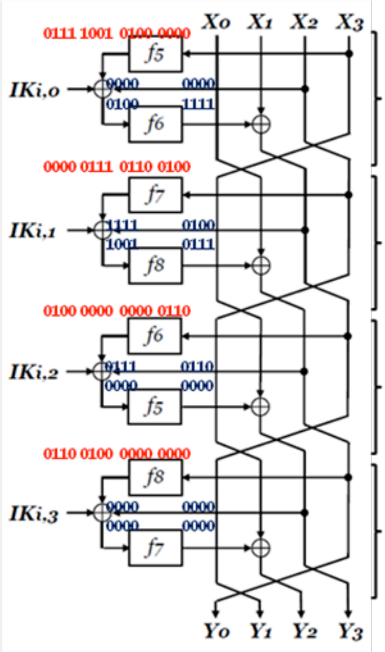


F2 Function (Cipher)

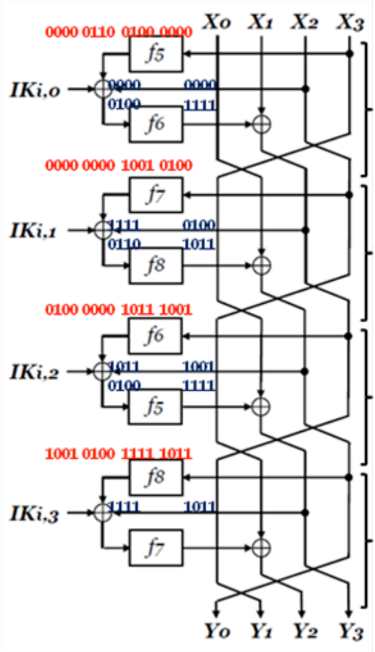
(1,1,0,0,0,0,1,0,1,1,1,1,1,0,1,1)



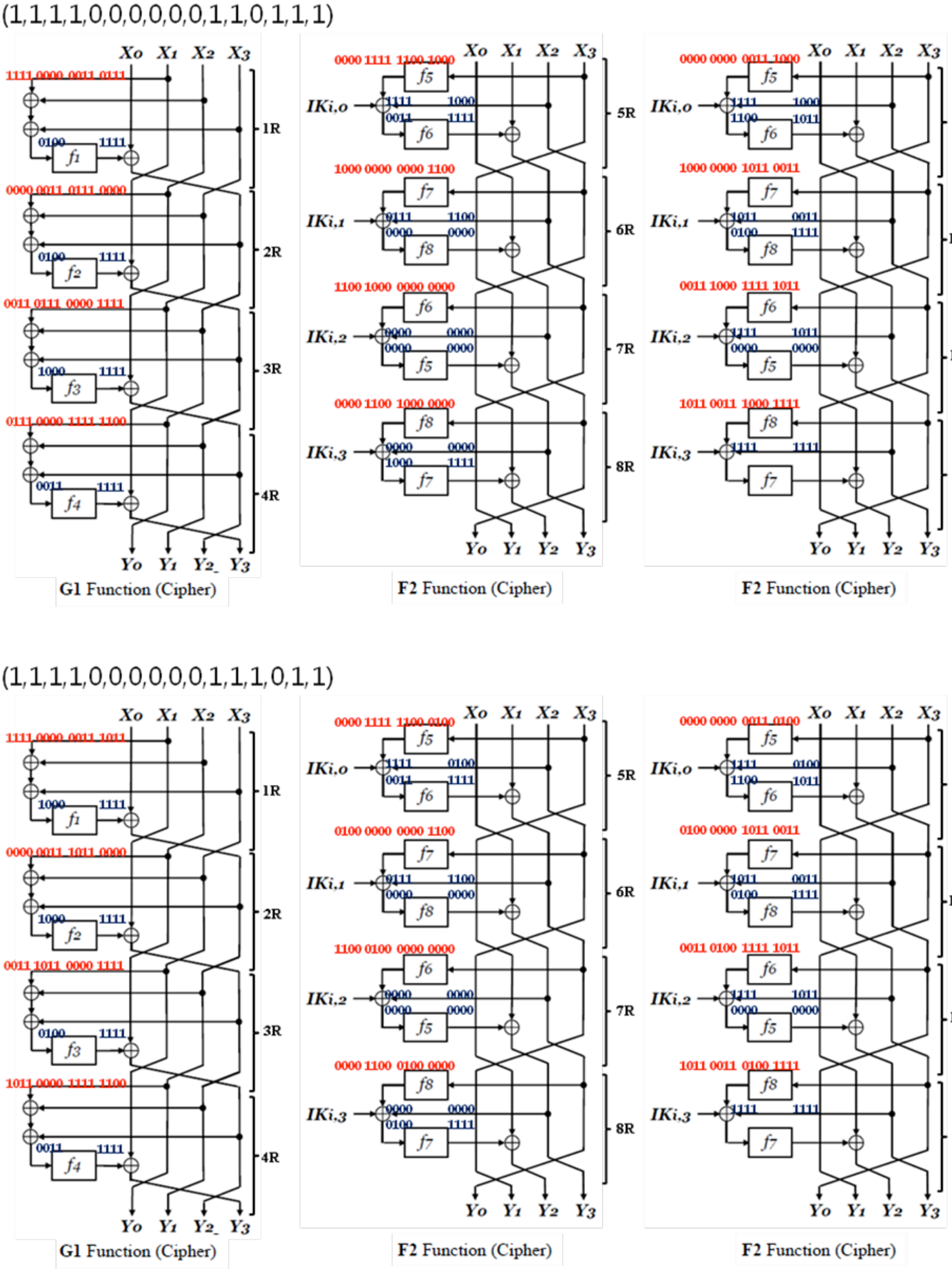
G1 Function (Cipher)



F2 Function (Cipher)



F2 Function (Cipher)


(1,1,1,1,0,0,0,0,0,0,1,1,0,1,1,1)

G1 Function (Cipher)

F2 Function (Cipher)

F2 Function (Cipher)

(1,1,1,1,0,0,0,0,0,0,1,1,1,0,1,1)

G1 Function (Cipher)

F2 Function (Cipher)

F2 Function (Cipher)

Figure 10 - differential propagations characteristic

3.2 Higher order differential cryptanalysis

Higher order differential cryptanalysis is effective in the cipher with nonlinear components which have low algebraic degree and less iterative rounds. The S-boxes of HyRAL have algebraic degree 7. Each output bit of the S-box can be regarded as a Boolean function with 8 input variables.

After three rounds the algebraic degree of any intermediate bit becomes 7^3. Thus, the number of plaintexts needed for higher order differential cryptanalysis using a 3 round distinguishers is greater than 2^{128}. So for only up to 2 round, distinguisher may be found for application of higher order differential cryptanalysis. Therefore, for 24 rounds(128-bit secret key) or 32 rounds(192-bit and 256-bit secret key) HyRAL, the algebraic degree of the ciphertexts as function of plaintexts is high enough to resist against a higher order differential cryptanalysis.

3.3 Impossible Differential Cryptanalysis

Impossible differential cryptanalysis is an attack finding right key by discarding wrong keys using differential trails with probability zero. Such differential trails are composed of two subtrails with probability 1 which cannot be connected.

At FIT2010, Shinayama, et. al., present a security evaluation result of HyRAL against impossible differential attacks[SIKH10]. They conclude that impossible differential attacks can be applied to 14-round HyRAL-128, 14-round HyRAL-192 and 15-round HyRAL-256, but are not effective for full round HyRAL.

We failed to find differential trails with probability 1 for more than 9 rounds and hence impossible differential trails for more than 18 rounds. It seems that 6R attack for HyRAL-128 and 14R attack for HyRAL-192/256 are not feasible. Therefore we think full round HyRAL-128 and HyRAL-192/256 are secure against impossible differential attacks.

3.4 Linear Cryptanalysis

3.4.1 Linear Cryptanalysis

Linear cryptanalysis is one of the most well-known and powerful approaches to attacking many block ciphers[M94]. This method considers linear relationships between the input and output.

It is known that the upper bound of linear characteristic probabilities can be estimated using the minimum numbers of linear active s-boxes in some consecutive rounds.

Definition 1 A linear active s-box is defined as an s-box given a non-zero output mask value.

Definition 2 For any given $\Gamma_x, \Gamma_y \in GF(2^m)$, the linear probabilities of $s_i - box: GF(2^m) \to GF(2^m)$ are defined as

$$Pr_x[x \cdot \Gamma_x = s_i(x) \cdot \Gamma_y] = \frac{\#\{x \in GF(2^m) | x \cdot \Gamma_x = s_i(x) \cdot \Gamma_y\}}{2^m}$$

and the linear probability of iterated block cipher f_i is defined to be

$$LP_{f_i}(\Gamma_x, \Gamma_y) = (2Pr_x[x \cdot \Gamma_x = s_i(x) \cdot \Gamma_y] - 1)^2.$$

Definition 3 Let q_s be the maximum linear probability of all s-boxes .

$$q_s = \max_i \max_{\Gamma_y \neq 0, \Gamma_x} LP_{f_i}(\Gamma_x, \Gamma_y)$$

Theorem 1 Let *L* be the minimum numbers of total linear active s-boxes. Then, the maximum linear characteristic probability is bounded by q_s^L .

Definition 4 Let $f_i = f_1 \circ f_2 \circ \cdots \circ f_r$ be an iterated block cipher made of *r* rounds. An *r*-round linear characteristic Γ_z is a sequence of masks defined as an

$$\Gamma_z = \left(\Gamma_{z^{(1)}}, \Gamma_{z^{(2)}}, \cdots \Gamma_{z^{(r)}}\right).$$

Definition 5 The linear characteristic probability of an *r*-round iterated function f_i relatively to an *r*-round linear characteristic Γ_z is defined as

$$LCP(\Gamma_z) = \prod_{i=1}^{r} LP_{f_i}(\Gamma_x, \Gamma_y).$$

Definition 7 The maximum linear characteristic probability is defined as

$$LCP_{max} = \max_{\Gamma_z, \Gamma_{z(i)} \neq 0} LCP(\Gamma_z).$$

With the above-mentioned techniques, we can show that HyRAL offers immunity to the linear attack by showing the upper bound of maximum linear characteristic probability, $LCP_{max} < 2^{-128}$.

3.4.2 Truncated Linear Cryptanalysis

Truncated linear cryptanalysis is a general technique for the analysis of block ciphers, which was proposed by the designers of Camellia[AIK$^+$00]. Truncated linear cryptanalysis uses '0' and '1' to represent each input and output byte data of S-boxes. In order to evaluate the immunity against linear cryptanalysis, the knowledge of the guaranteed numbers of linear active S-boxes and maximum linear probability of S-boxes can be used. Truncated linear cryptanalysis of HyRAL was achieved by Igarashi *et al*. [ITK10]. They searched the number of linear active S-boxes through the Viterbi algorithm and computed the maximum linear characteristic probability $\mathrm{LCP}_{\max}$.

Table 2 and Table 3 show the numbers of active S-boxes of HyRAL-128 and HyRAL 192/256, respectively.

Table 2 -Numbers of Linear Active S-boxes for HyRAL-128

round	# of active S-boxes	round	# of active S-boxes
1	0	13	22
2	1	14	22
3	1	15	22
4	2	16	27
5	7	17	32
6	7	18	32
7	7	19	37
8	7	20	37
9	12	21	37
10	12	22	37
11	17	23	37
12	22	24	38

Table 3- Numbers of Linear Active S-boxes for HyRAL-192/256

round	# of active S-boxes	round	# of active S-boxes
1	0	17	31
2	3	18	31
3	6	19	31
4	6	20	31
5	6	21	36
6	6	22	41
7	6	23	41
8	11	24	46
9	11	25	46
10	16	26	46
11	21	27	46
12	21	28	51
13	21	29	52
14	21	30	52
15	26	31	53
16	26	32	53

Combining 38 active S-boxes for HyRAL-128 and S-box property, the maximum linear characteristic probability $\mathrm{LCP}_{\mathrm{max}} \leq 2^{-6\times 38} = 2^{-228}$. The maximum linear characteristic probability of HyRAL-192/256 $\mathrm{LCP}_{\mathrm{max}} \leq 2^{-6\times 53} = 2^{-318}$.

We conclude that it may be very difficult for an attacker to find full round linear-hulls which can be used to distinguish HyRAL from random permutations.

3.5 Related-Key Attack

3.5.1 Related-Key Differential Attack

Related-key cryptanalysis was proposed by Biham[B94]. This attack considers the information that can be extracted from two encryptions using related keys. The concept was used in [KSD97] to present the idea of related-key differentials. These differentials study the development of differences in two encryptions under two related keys.

A related-key differential is a triplet of a plaintext difference ΔP, a ciphertext difference ΔC, and a key difference ΔK, such that

$$\Pr_{P,K}[E_K(P) \oplus E_{K \oplus \Delta K}(P \oplus \Delta P) = \Delta C]$$

is high enough (or zero).

L is a ciphertext by HyRAL-128. Takagi *et al.* searched the number of differential active S-boxes by the Viterbi algorithm[TIK10]. Table 3 shows that HyRAL-128 has at least 37 active S-boxes, and we have $DCP_{max} \leq 2^{-6\times 37} = 2^{-222}$. Therefore, for any ΔK and ΔL, a differential probability of $(\Delta K \rightarrow \Delta L)$ is expected to be less than 2^{-128}, i.e., no useful differential $(\Delta K \rightarrow \Delta L)$ exists. This implies the probability of any related-key differential $(\Delta P, \Delta C, \Delta K)$ is less than 2^{-128}.

For 192 and 256-bit keys, $L_{192/256}$ is generated by HyRAL-192/256. Table 4 shows that HyRAL-192/256 has at least 57 differential active S-boxes, which implies there are no differential characteristic with probability more than 2^{-128}. That is, for any $\Delta K_{192/256}$ and $\Delta L_{192/256}$, a differential probability of $\Delta K_{192/256} \rightarrow \Delta L_{192/256}$ is expected to be less than 2^{-128}. Therefore, the probability of any related-key differential $(\Delta P, \Delta C, \Delta K_{192/256})$ is less than 2^{-128}.

Therefore, we conclude full-round HyRAL-192/256 is strong enough against related-key cryptanalysis.

Table 4 - Numbers of Differential Active S-boxes for HyRAL-128

round	# of active S-boxes	round	# of active S-boxes
1	0	13	23

2	1	14	28
3	1	15	29
4	1	16	30
5	6	17	30
6	7	18	30
7	12	19	35
8	12	20	36
9	12	21	36
10	13	22	37
11	14	23	37
12	19	24	37

Table 5- Numbers of Differential Active S-boxes for HyRAL-192/256

round	# of active S-boxes	round	# of active S-boxes
1	0	17	28
2	0	18	33
3	1	19	37
4	1	20	39
5	2	21	40
6	7	22	48
7	7	23	49
8	7	24	50

9	8	25	50
10	9	26	50
11	14	27	55
12	18	28	56
13	22	29	56
14	23	30	57
15	28	31	57
16	28	32	57

3.5.2 Related-Key Boomerang attack

The relate-key boomerang attack is a combination of the boomerang technique with the related-key differential technique. The main idea behind the attack is to use two short related-key differentials with high probabilities instead of one long related-key differential with a low probability. The motivation for such an attack is that it is easier to find short differential with high probability than to find a long differential with high enough probability in many block ciphers [BDN05].

Let *n* be the block size in bits and *k* be the key length in bits. As in the case for the boomerang attack, we assume that HyRAL $E: \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$ can be described as a cascade, i.e., $E = E_1 \circ E_0$, such that for E_0 there exists a related-key differential $\alpha \rightarrow \beta$ under a key difference ΔK_0 with probability p, and for E_1 there exists a related-key differential $\gamma \rightarrow \delta$ under a key difference ΔK_1 with probability q.

The related-key boomerang process involves four different unknown (but related) keys : K_a, $K_b = K_a \oplus \Delta K_0$, $K_c = K_a \oplus \Delta K_1$, and $K_d = K_a \oplus \Delta K_0 \oplus \Delta K_1$. The attack is performed by the following algorithm:

- Choose a plaintext P_a at random and compute $P_b = P_a \oplus \alpha$.
- Ask for the encryption of P_x under K_x, i.e., $C_a = E_{K_a}(P_a)$ and $C_b = E_{K_b}(P_b)$.
- Compute $C_c = C_a \oplus \delta$ and $C_d = C_b \oplus \delta$.

- Ask for the decryption of C_x under K_x, i.e., $P_c = E_{K_c}^{-1}(C_c)$ and $P_d = E_{K_d}^{-1}(C_d)$.
- Test whether $P_c \oplus P_d = \alpha$.

It is easy to see that for a random permutation the probability that the last condition is satisfied is 2^{-n} . For E the probability that this condition is satisfied is p^2q^2 just like for a regular boomerang attack, and we need $(pq)^2 > 2^{-128}$, i.e., $pq > 2^{-64}$, in order to attack HyRAL. All possible values for p and q can be derived from Table 4 and Table 5. HyRAL-128 with at most 12 rounds, and HyRAL-192/245 with at most 13 rounds can be distinguished from a random permutation. It is hard to achieve the condition, $pq > 2^{-64}$.

Therefore, we conclude that the attack is unlikely to be any threat to HyRAL.

3.6 Weak Key

The strength of the encryption function $E_k(P)$ may differ significantly for different keys *K*. If for some set of keys the encryption function is much weaker than for the others this set is called a class of weak keys. The attack technique that succeeds against the keys in the class of weak keys is called a membership test for the class. For example, if the test uses differential cryptanalysis, then it will be called a *differential membership test*.

Assume the key space has *K* bits, so that complexity of exhaustive search is 2^k. Assume there exists a class of weak keys of size 2^f, with a complexity of the membership test of 2^w. If $2^w < 2^f$ exploiting weak keys is more efficient than using the exhaustive search.

The key schedule algorithm of HyRAL uses only large functions G_1, G_2 to computes subkey RK_i and intermediate key IK_i. Tkagi *et al.* shows the numbers of differential/linear active S-box of each f_i [TIK10] [ITK10]. From their results, we can find that G_1 and G_2 have smaller active S-boxes than F_1, F_2. The simple use of large functions for key schedule may induce some weaknesses. We consider that there may exist attacks such as DCP or LCP > 2^{-128}. Asano *et al.* show that the weak keys for 256-bit key HyRAL by differential membership test with complexity $2^{48.8}$[AYI11]. They show that 256-bit Key HyRAL has 2^{51} weak keys.

Round key RK_i and intermediate Key IK_i is derived from KM_i. We observe that the building block of KM_i is similar to iterated hash function which has the simple chaining structure. It implies that there is possibility that some cryptanalysis techniques against hash functions can be applied to key schedule algorithm.

Therefore we doubt the existence of weak keys.

3.7 Interpolation Attack

The interpolation attack was proposed by T. Jakobsen and L.R. Knudsen at FSE 97 as a reaction to ciphers using algebraically constructed S-Boxes such as those proposed by Nyberg at EUROCRYPT 93. In fact, interpolation attacks were the first demonstration of successful polynomial-based algebraic attacks against block ciphers. Interpolation attacks work by expressing the relationship between the plaintext and ciphertext for a fixed key as either one or as a vector of polynomials.

If the degree of these polynomials is low enough, the coefficients of the polynomials can be interpolated from a number of plaintext/ciphertext pairs. A key-dependent equivalent of the encryption or the decryption algorithm has then been determined. In general, this number increases exponentially with the degree of the polynomial function describing the S-box, the number of rounds and the number of elements in the internal state.

Since HyRAL provides “full diffusion” after only one round, so it can be considered resistant against the interpolation attack.

3.8 Algebraic Attack

The Advanced Encryption Standard (AES), in contrast to many other block ciphers like DES, is very simple and algebraically clean. The S-box is the unique nonlinear part of AES and it is just a patched inverse in GF(2^8). Based on the structure of the S-box, Courtois and Pieprzyk reformulate AES as a system of Multivariate Quadratic equations (MQ) over GF(2) . If the quadratic system can be solved faster than exhaustive key search, the AES is broken.

There is much discussion and speculation about whether such algebraic attacks might ever be relevant. While some very positive views have been expressed, most researchers are more cautious. Without doubt, the need to find powerful elimination techniques for multi-variate equation systems is a significant topic in cryptography, though not only in the context of block ciphers. Some well known basic ingredients such as linearization (substitution of monomials by single new variables) and Buchberger’s algorithm (computations of Groebner bases), have lead to algorithms such as XL (eXtended Linearization), XSL (eXtended Sparse Linearization), and also the algorithms F4 and F5 due to Faugere. Unfortunately the complexity of these algorithms is closely related to very difficult problems in algebraic geometry and commutative algebra, and heuristics are very risky.

So far, no attacks were successful for block ciphers using AES type round functions. The round function of HyRAL is also AES type.

Therefore, we could conclude that HyRAL and AES are in the same basket of eggs for the vulnerability of algebraic attacks.

4 Survey of previous results

The only previous result on HyRal that we are aware of is that in [TIK10].

References

[AIK+00] K. Aoki, T. Ichikawa, M.Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita, "Camellia: A 128-bit block cipher suitable for multiple platforms," 2000. Available at http://info.isl.ntt.co.jp/crypt/camellia/dl/support.pdf.

[AYI11] Y.Asano, S.Yanagihara, nd T. Iwata, " Equivalent keys of 256-bit key HyRAL," SCIS2011.

[B94] E.Biham, "New Types of Cryptanalytic Attacks Using Related Keys," *Journal of Cryptology*, Vol.7, No.4, pp.229-246, 994.

[BDN05] E.Biham, O, Dunkelman, and N.Keller, "Related-Key Boomerang and Rectangle attacks," *Advances in Cryptology*-EUROCRYPT'05, pp.507-525.

[BNPV02] A. Biryukov, J.Nakahara Jr, B.Preneel, J.Vandewalle, "New Weak-Key Classes of IDEA," ICICS 2002, pp.315-326.

[CP02] N. Courtois and J. Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In Advances in Cryptology - ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages pp. 267 – 287. Springer Verlag Heidelberg, 2002.

[ITK10] Y. Igarashi, Y. Takagi, and T. Kaneko, " Security evaluation of HyRAL against linear cryptanalysis," SCIS 2010.

[JK97] T. Jakobsen and L.R. Knudsen. The interpolation attack on block ciphers. In E. Biham, editor, Proceedings of Fast Software Encryption 1997, LNCS 1267, pages 28–40, Springer-Verlag, 1997.

[KSD97] J.Kelsey, B.Schneier, and D.Wagner, “Related-key cryptanalysis of 3-way, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA.” In proceedings of Information and Communication Security’97, no. 1334 in LNCS, pp.233-246, Springer-Verlag, 1997.

[M94] M. Matsui, “Linear Cryptanalysis Method for DES Cipher,” *Advances in Cryptology*-EUROCRYPT’93, pp.386-397.

[N94] K. Nyberg. Differentially Uniform Mappings for Cryptography. In Advances in Cryptology - EUROCRYPT ’93, volume 765 of Lecture Notes in Computer Science, page pp. 55 ff. Springer Verlag Heidelberg, 1994.

[TIK10] Y.Takagi, Y.Igarashi, and T. Kaneko, “Security evaluation of HyRAL against differential attack,” SCIS 2010, IEICE, 2010.