A Design of Block cipher-Secure Electronic Xenogenesis Algorithm for Efficient Plaintext Management in Block Cryptosystem

Seon-Keun Lee*, Hwan-Yong Kim** ***Regular Members***

ABSTRACT

Presently, network is being in the existence as an influence can not be neglected. This rapid progress of network has gone with development of mobile network and information communication. But the development of network can generate serious social problems. So, it is highly required to control security of network. These problems related security will be developed and keep up to confront with anti-security part such as hacking, cracking. There's no way to preserve security from hacker or cracker without developing new cryptographic algorithm or keeping the state of anti-cryptanalysis in a prescribed time by means of extending key-length. Worldwidely, many researchers for network security are trying to handle these problems.

In this paper, we proposed a new block cryptosystem. The Block cipher-Secure Electronic Xenogenesis Algorithm(B-SEXA) which is capable to cipher regardless of key distribution or key-length for these definite problem is proposed and designed in hardware. B-SEXA increase secret level from using a nonlinear function in multiply for key data utilized in cryptography and feistel structure that generates MDP and MLP in maximum is proposed to prevent cryptography analysis. The designed B-SEXA in this paper performed synthesization and simulation using Synopsys Ver. 1999.10 and VHDL.

Key words: Block cryptosystem, cryptography, VLSI, VHDL

Ⅰ. Introduction

The rapid growth of mobile-network and wireless-network causes a development of computer-network and generate a problem related to security at the same time. To solve this security problem, new cipher algorithm and compensation method for key strength has been risen and developed. But these methods which has been studied in mathematical way contain a problem such as difficulty in realization or reveal to hackers, so realization and putting to practical use of cryptographic algorithm contain lots of problem. To preserve security from hacker, extending of key strength may be little free from security problem, but it can't be absolute key to many security problem.[1][2][3]

Also, in case of extending a key strength in with no limit, encipherment and decipherment time will become longer and cause inconvenience to users joined.[4]

In this paper, the Block cipher-Secure Electronic Xenogenesis Algorithm(B-SEXA) which is capable to cipher regardless of key distribution or key-length for these definite problem is proposed and designed in hardware.

B-SEXA increase secret level from using a nonlinear function in multiply for key data utilized in cryptography and modified feistel structure that generates MDP and MLP in

* Dept. of Electronics Engineering Wonkwang University(caiserrisk@korea.com)
** Dept. of Electronics Engineering Wonkwang University

논문번호 : 020025-0121, 접수일자 : 2002년 01월 21일
※ 정보통신부에서 지원하는 대학기초연구지원사업으로 수행(과제번호 2001-119-2)

maximum is proposed to prevent cryptography analysis. B-SEXA generate electrical xenogenesis by means of increasing nonlinear characteristics in nonlinear function so non-authenticator who has a specific key value or ciphertext can't accomplish decipherment using DC (differential cryptanalysis) or LC(linear cryptanalysis) methods.

Also key exhaustive search method can not be performed as a cracking as different outputs are generated whenever key exhaustive search is tried.[5]

B-SEXA fundamentally reinforces protection for DC or LC from using s-box which express nonlinear characteristics in DES in multiple and modified feistel structure which change basic structure in block cryptosystem.

II. Secret Cryptosystem

Secret cryptosystem which of encipherment and decipherment key is equal connect directly with keeping or distribution of key as safely. Secret cryptosystem encipher and decipher data in block or stream and block cryptosystem includes authentication besides encipherment. Block cryptography is a representative cryptography of cryptosystem which perform encipherment by way of block-unit in fixed size using plaintext data. DES, FEAL, LOKI, IDEA, SAFER, and RC has been proposed in block cryptographic algorithm.[1][2][3][4][8][11]

Block cryptography consists of feistel, S-P(substitution and permutation) and hybrid method which is mixed two methods.

DC which is proposed in 1990 method has been well known as the most strong method to impotent block cryptosystem. DC is more effective than key exhaustive search and seriously has an influence on block cryptosystem with feistel structure from characteristic of DC itself. DC delivers an attack ciphertext by means of the fact that the difference of data in front of rear of combination is equal in each other, that is, DC is a method to utilize chosen ciphertext attack.

$$\begin{aligned}(X\otimes K)\otimes(X'\otimes K)^{-1}&=X\otimes K\otimes K^{-1}\otimes X'^{-1}\\&=X\otimes(X')^{-1}=\Delta X\end{aligned}\qquad(1)$$

As seen in equation (1), DC gives a key to interpret block ciphertext using difference value, ΔX. So, DC gets cipher-pair according to P' from P and ΔP based on difference characteristic of $(\gamma-1)$ round.[6][7]

After obtaining cipher-pair, get the candidating key K_r' from cipher-pair, and final out real round K_r, To obtain K_r, above process be repeated.

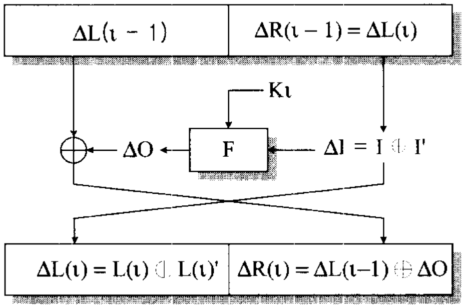


Fig. 1 The differential characteristic

In case, difference input ΔI for input (I, I') exists and we know the difference output ΔO, we can calculate candidating key K_r.

Equation (2) denotes DP(differential probability) and MDP(maximum differential probability) for i-th round by means of DC method.[9]

$$\begin{aligned}DP &= P(\Delta Y(i)=\beta \mid \Delta X(0)=\alpha)\\&=\sum_{\Omega_\Lambda}P(\Omega_P=\alpha,\ \ \Omega_\Lambda,\Omega_T=\beta)\\MDP &= \max{}_\beta\max{}_\alpha P(\Delta Y(i)=\beta \mid \Delta X(0)=\alpha)\end{aligned}\qquad(2)$$

LC proposed in 1993 uses a known plaintext attack method.

$$(P\cdot\alpha)\oplus(C\cdot\beta)=(K\cdot\gamma)\qquad(3)$$

This attack method that utilizes the linear approximation among plaintext, ciphertext and key use linear approximation such as equation (3) in case $\max|P_L - 1/2|$ for every key.

LC finds out the whole key information from expanded one-bit key information that gets the key information in cases of $T > N/2$ then $K \cdot \gamma = 0$ and $T < N/2$ then $K \cdot \gamma = 1$ based on linear approximation T for whole plaintext P and ciphertext C.

$$\begin{aligned} MDP_m &\triangleq Max_{\Delta X \neq 0,\, \Delta Y} DP(\Delta X \rightarrow \Delta Y) \\ MLP_m &\triangleq Max_{\Gamma X,\, \Gamma Y \neq 0} LP(\Gamma X \rightarrow \Gamma Y) \end{aligned} \tag{4}$$

Equation (4) shows the MDP for DP in equation (2) and MLP for LP, respectively.

That is, to obtain MDP and MLP for DP and LP, it is required to enlarge the relation $\Delta X \rightarrow \Delta Y$ and $\Gamma X \rightarrow \Gamma Y$. In this paper, we propose B-SEXA to increase nonlinear characteristic and rise the secret level of block cryptosystem by means of that.[4][10]

Ⅲ. Block-cipher Secure Electronic Xenogenesis Algorithm

The most important things in designing block cryptosystem are confusion and diffusion. Massey, cryptanalyst, defined that ciphertext is kinds of what the statistics of ciphertext is highly complex to plaintext's in attacker and diffusion is sufficient influencing from each bit of plaintext and key to each bit of ciphertext.

But confusion and diffusion defined by Massey requires the condition that the ciphertext must be decipherment in perfect. So, confusion and diffusion are restricted within perfect decipherment.

This restriction causes a problem that anti-authenticators can be decipher the ciphertext. So, hacking and cracking by means of the theory of possibility and statistics may be occur. Also, it means authenticator spend lots of expense to get the information.

These facts can cause waste of resources and drop of efficiency of network and furthermore, degenerate the development of information communication.

B-SEXA is somewhat different in confusion and diffusion defined Massey from above reasons. That is, it does not require complicated type of confusion and influence to each bit of ciphertext from each bit of plaintext and key. Almost perfect confusion and diffusion means that the hacker gets the chance to approach certain information.

B-SEXA adjust the focus of increasement of nonlinear characteristic and modified feistel structure.

Many researches for feistel structure itself against DC and LC have developed.

But these studies about feistel structure are only a way of protection against DC and LC, we can't expect secret level increasing of overall encipherment in study. From these reasons, B-SEXA proposed in this paper uses two nonlinear function s-box, and modified feistel structure in order to protect block cryptosystem in safe against DC and LC.

Generally, the performance of s-box is evaluated in measurement of decreased amount of uncertainty in unknown output from partial information about input or output of s-box.

The rules of s-box in cryptosystem, DES which uses s-box is below

R0. Each column of s-box is substitution to an integer(even : 0~15, odd : 0~15)

R1. All s-box is not only linear but also affine function.

R2. More than two bit of output will be changed in the case of the one is changed among 6-input bit of S-Box.

R3. S(x)와 S(x ⊕ 001100) must be changed at least two bit.

R4. S(x) ≠ S(x ⊕ 11αβ00) for arbitrary α,β.

R5. s-box in the all output must be selected the smallest in the difference of the number of 0 and 1 (that is to say, weight is the minimum) in case of one bit is fixed.

In designing s-box, choose of design criterion of s-box take a cautious attitude.

So, it means that lots of conditions are required about DC and LC which are successful attack way to DES.

LC must consider nonlinearity of s-box as using linear approximation of s-box and design of s-box must guarantee the avalanche because DES is a kind of S-P network.

Second, permutation condition in composition of 6×4 s-box must be considered. Following conditions are related in permutation.

CP0. 4-bit input boolean function which forms substitution is nonlinear.

CP1. More than two bit of output will be changed in the case of the one is changed among 4-input bit.

CP2. G(x)와 G(x ⊕ 0110) must be changed at least two bit.

CP3. 0.25 $\leq P^{G}_{ij}$ $\leq$0.75, $0 \leq i$, $j \leq 4$ in considering avalanche

CP4. $\left| P\{ Y_j = \beta \mid X_i = \alpha \} \right| - \frac{1}{2} \leq \frac{1}{8}$,

$(0 \leq i,\ j \leq 4)$, $(\alpha, \beta \in Z_2)$

CP5. Information leakage of each case of above(CP1~CP4) is less than maximum information leakage of DES substitution.

This permutation has limitation condition as following.

C1. $\mathrm{wt}(G_0(x) \oplus G_1(x)) \geq 2$

$\mathrm{wt}(G_0(x) \ominus G_2(x)) \geq 2$

$\mathrm{wt}(G_1(x) \ominus G_3(x)) \geq 2$

$\mathrm{wt}(G_2(x) \ominus G_3(x)) \geq 2$

C2. $G_0(x) \neq G_2(x \oplus 1efg)$ $e, f, g \in Z_2$

$G_1(x) \neq G_3(x \oplus 1efg)$ $e, f, g \in Z_2$

where, i range of G_i is $0 \leq i \leq 3$

The procedure of s-box in condition of restrictions and conditions mentioned previously.

i) G_i must satisfy the every condition(CP 1~CP4).

ii) G_i is conformed by R1 and R2 in turn.

Figure 2 shows modified type of s-box which is composed of combination of s-box in multiple. If increasement of complexity of nonlinear function in s-box function in figure 2, the range of equation (4) will become grow.

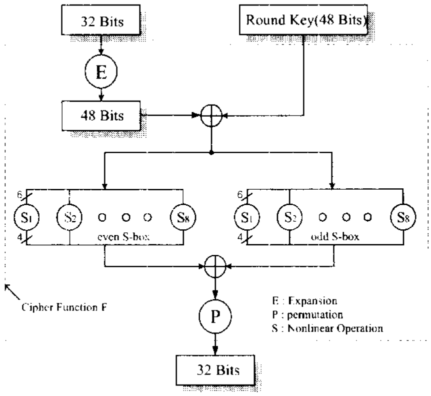


Fig. 2 F function including multiple s-box

The studying for feistel structure are vigorous and 7 kinds of structure for way of protection against DC or LC are exist generally(type B, type L, type R, type LB, type RB, type LR, type LRB). In these structure, equation (5) denotes stability for DP or LP and B type feistel structure in figure 3 has the best secret level and is easy to realization in general.

$$\begin{aligned} &DP_B < DP_L = DR_{RB} \le DP_{LB} = 2DP_B, \\ &2DP_B < DP_{LR} = 2DP_L < DP_{LRB} = 3DP_B \\ &LP_B < LP_L = LR_R < LP_{RB} = 2LP_B, \\ &2LP_B < LP_{LR} = 2LP_L < LP_{LRB} = 3LP_B \end{aligned} \qquad (5)$$

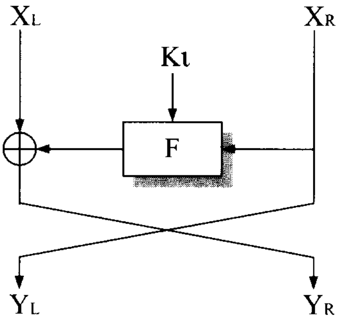


Fig. 3 The B type feistel structure

The improvement of stability for feistel has the better secret level than any other type when the type B such as nDP_B, nLP_B is chosen which is shown in equation (5) and figure 3.

Feistel cryptosystem is a structure that generates m-bit ciphertext for 2m-bit plaintext in the procedure r-round and equation (6) shows the procedure. where, $r \ge 1$, For $1 \le i \le r$.

$$L_i = R_{i-1}\ ,\quad R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \qquad (6)$$

In this paper, we transform feistel structure as figure 4 because feistel structure in equation (6) has a very strong possibility to be exposed by DC characteristic

The structure in figure 4, actualizes reinforce and realization of security strength and moreover makes possible to handle feistel structure in parallelism.

It assures the same degree of secret level and security strength as the existing cryptosystem as just 8 times of repeated operation without 16 round in rounding.

The proposed B-SEXA system accomplishes security strength of existing system, and also guarantees the stability against DC attacks.

Namely, it obtains MDP and MLP for nDP_B, nLP_B like equation (5) without any special signal process. That is to say, B-SEXA is a structure that gets rid of the characteristics of DC or LC for feistel structure. where, ⊗ : 32-bit ex-or operation part, ⊠ : 32-bit ex-nor operation part.

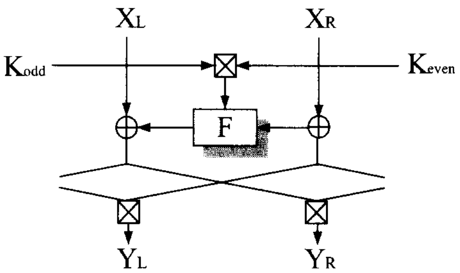


Fig. 4 Feistel structure of modified B type

Equation (7) shows the generated equation for feistel structure of proposed B-SEXA, and we can see no difference with single feistel structure

However, B-SEXA preserves high secret level as having the ⊠ function which keeps the secret level highly though it is fitted by existing feistel structure.

Actually, it is very difficulty to distinguish the original value from result value though the calculating result between ⊗ and ⊠ is opposed to each other in the aspect of secret level in cryptography.

When the ⊗ and ⊠ are used in parallel, it has one way characteristic such as hash function so the analysis of data by anti-authenticator with DC and LC will be more difficult.

In comparison with equation (6) and (7), the change width of equations is one-round in equation (6) but equation (7) brings 2-round in the while of rounding.

One rounding procedure in B-SEXA executes the same role 2-rounding in the feistel structure.

Therefore, B-SEXA produce twice processing gain as compared with rounding itself at some condition.

$$\begin{aligned} L_n &= R_{n-2} \oplus F[(k_n \boxtimes k_{n+1}), L_{n-1} \\ &\quad \oplus F[k_{n+1}, R_{n-2}]] \\ R_n &= L_{n-2} \oplus F[k_n, F[(k_n \boxtimes k_{n+1}), L_{n-1} \\ &\quad \oplus F[k_{n+1}, R_{n-2}]]] \\ &= L_{n-2} \oplus F[k_n, L_n] \end{aligned} \tag{7}$$

The relation between equation(6) and equation (7) are same as equation (8).

$$\begin{aligned} &DP_B \langle \cdots \langle 2DP_B \langle \cdots \langle 3DP_B \langle \cdots \langle nDP_B \\ &LP_B \langle \cdots \langle 2LP_B \langle \cdots \langle 3LP_B \langle \cdots \langle nLP_B \end{aligned} \tag{8}$$

The purpose of proposed B-SEXA is preservation of data with high secret level against DC and LC by means of using feistel structure and increasing nonlinear characteristics of s-box.

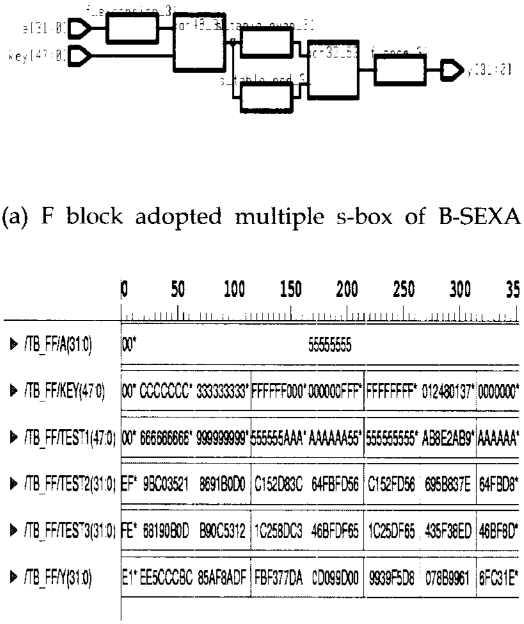
Ⅳ. The hardware design of block cryptosystem with proposed B-SEXA

To increase the range of equation (4), in figure 5(a), we combine nonlinear function s-box in multiple like figure 2.

Figure 5 shows the realization of multiple s-box proposed B-SEXA using VHDL coding and synopsys tool. Here, we define s-function in even and odd case of the inside of s-box in figure 2 and then calculate the output with mutual exclusive-or logic.

We chose the same structure with existing structure in order to increase the MDP and MLP for f-function and multiple s-box with 2 s-box.

The each output of multiple s-box performs bit-by-bit exclusive-or and let out the output. Figure 5(b) shows the outputs of this function.


key[47:0]
0
50
100
150
200
250
300
35
/TB_FF/A(31:0)
00*
55555555
/TB_FF/KEY(47:0)
00* CCCCCCC* 333333333* FFFFFF000* 000000FFF* FFFFFFFF* 012480137* 0000000*
/TB_FF/TEST1(47:0)
00* 666666666* 999999999* 555555AAA* AAAAAA55* 555555555* AB8E2AB9* AAAAAA*
/TB_FF/TEST2(31:0)
EF* 9BC03521 8691B0D0 C152D83C 64FBFD56 C152FD56 695B837E 64FBD8*
/TB_FF/TEST3(31:0)
FE* 68190B0D B90C5312 1C258DC3 46BFDF65 1C25DF65 435F38ED 46BF8D*
/TB_FF/Y(31:0)
E1* EE5CCCBC 85AF8ADF FBF377DA CD099D00 9939F5D8 078B9961 6FC31E*

(a) F block adopted multiple s-box of B-SEXA

(b) Simulation results of F block adopted multiple s-box of B-SEXA

Fig. 5 F block adopted multiple s-box of B-SEXA

32 bits input and 48 bits key value(data) accomplish exclusive-or logic and the output of them are used in the input of even and odd function of s-box.

TEST1 in figure 5(b) shows the result of exclusive-or and TEST2 and TEST3 shows the result of even and odd of s-box, respectively.

The final ouput of multiple s-box is 32 bits Y.

So, the final output of multiple s-box is result of exclusive-or between TEST2 and TEST3.

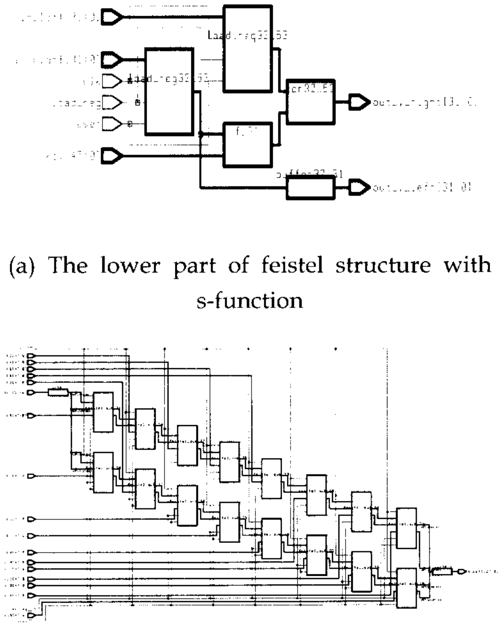
We can know in the figure 5(b) that the values by TEST2 and TEST3 have more transition than existing single s-box. That is to say, MDP and MLP increase in value.

Table 1 makes a list of mutual difference of the final output between f-function based on multiple s-box and single s-box. Here, exclusive-or for even and odd of s-box are used for the increasing secret level.

Table 1. Comparing mutual outputs of

existing and proposal s-box in F function

ODD-F	EVEN-F	Operation	B-SEXA-F
44C0C1EC	AA9C0D50	Exclusive OR	EE5CCCBC
87919254	023E188B		85AF8ADF
31A301F3	CA507629		FBF3777DA
3BE4EBAF	36ED76AF		0D099D00
3BE083F3	A2D9762B		9939F5D8
CB4A6DAE	CCC1F4CF		078B9961
31E668AF	5E2576AD		6FC31E02
31AF69AE	5C6C74AD		6DC31D03
30A749AF	5E6456A9		6EC31F06
35B729BF	5E7476BD		6BC35F02

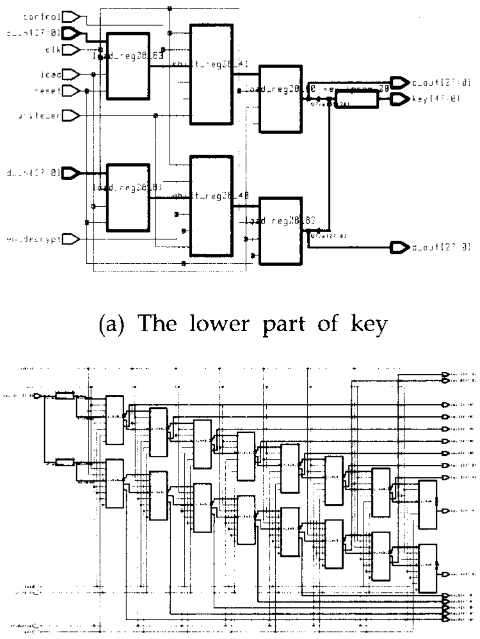


(a) The lower part of feistel structure with s-function

(b) Total feistel structure

Fig. 6 The structure of feistel with multiple s-function

Figure 6 shows the structure of feistel using multiple s-box. Figure 6(a) shows the lower part of structure of feistel including f-function consist of multiple s-box. To perform round operation, the lower part of feistel structure forms the whole feistel structure. Figure 6(b) shows the modified B-type feistel structure in order to B-SEXA, herewith, the structure of feistel by means of B-SEXA obtains the same secret level of 16 round with 8 round.



(a) The lower part of key

(b) Total key structure

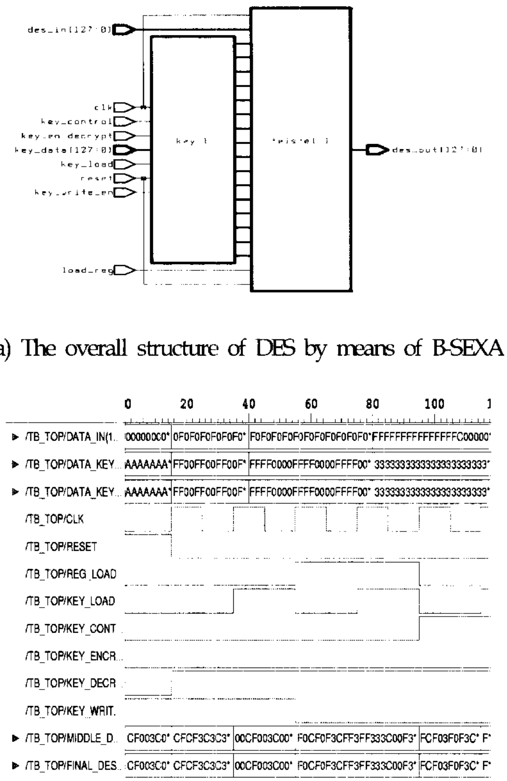
Fig. 7 Key structure for B-SEXA

Figure 7 shows the structure of key creating which is inevitable to modify because of changed B-type feistel structure.

This is a kind of modified structure in order to perform 8 round operation for accomplish 8 round in feistel structure. Figure 7(a) has the same a existing key generating structure and figure 7(b) shows the modified structure in lower part from 7(a) to perform 8 round operation.

Figure 8 shows the new block cryptosystem by means of the proposed B-SEXA which is modified from representative block cryptosystem, DES. Figure 8(a) is made up of key generating part and feistel structure and includes s-box and feistel structure like figure 4 in order to apply B-SEXA into feistel structure. Figure 8(b) indicates the final simulation result of block cryptosystem which is designed with proposed B-SEXA.

As we know figure 8(b), 128 bits FINAL_DES is generated from block encipherment using 128 bits data and key.



(a) The overall structure of DES by means of B-SEXA

(b) The simulation results of DES with B-SEXA

Fig. 8 Block cryptosystem with B-SEXA

In comparison with input data and ciphered output data, we can know that encipherment is similar to input value without occurring confusion and diffusion as Massey insist on.

Namely, it bring out more safe result than DC or LC which attacks plaintext which of a part is known or a selected portion part.

It means cryptographic algorithm with the proposed B-SEXA applied to block cryptosystem is more safe than existing key length increasing method for ciphertext attacking method using a defect of feistel structure without any key length increasement.

Table 2 compares and analyzes the difference between existing block cryptosystem, DES and DES by means of proposed B-SEXA.

The table 2 lets us know that DES using B-SEXA is higher twice in processing rate though the number of gate increases into 4/3 than existing cryptosystem using 16 round in the same condition.

Table 2. Comparing gate count and processing rate for existing and proposal DES

Existed and Proposal Block Cryptosystem		Gate counting	Processing method	Processing rate (@40㎒)

DES using unit round with control block	Existed	1,090	feedback after
			1 round processing
			16 round iteration
				416kbps(64bits)
				832kbps(128bits)

DES using 16th round		6,159	- each 16th processing	416kbps(64bits)
				832kbps(128bits)

DES using B-SEXA	Proposal	9,204	- 8 round processing simultaneously left and right block processing	833kbps(64bits)
				1.66Mbps(128bits)

V. Conclusion

In this paper, we proposed new block cryptosystem. The block cryptosystem by means of B-SEXA is proposed to expect more fast performance of network, more safe stability and integrity of network in accomplishing lots of high technical role of network caused by the development of information communication and rapid spreading internet.

B-SEXA enlarges the MDP and MLP in order to secure data from attacking of DC or LC and not utilize the existing key length increasement method to secure data.

Recently, trials to secure data in safe from DC or LC have been tried but they does not effective.

The proposed B-SEXA uses multiple

nonlinear s-box which increases nonlinearity and modified feistel structure in order to secure more safe data communication to authenticator without any inefficiency tried in existing method.

It decreases the process of rounding in existing block cryptosystem into 1/2 times which has trade-off relation between data processing time and data security and increases the performance of data process by way of one-time handling for heavy data. However, it more free from attacking of DC and LC by increasing MDP and MLP.

Worldwidely, many countries try to develope new cryptographic algorithm to deal with rapid growing information communication in actively in order to step into strong nation in information communication.

As mentioned reasons above, the proposed B-SEXA can bring up the solutions for a problem of organizing structure such as DES or SEED, FEAL, etc.

REFERENCES

[1] Shoji Miyaguchi, "The FEAL cipher family", In Alfred J. Menezes and Scott A. Vanstone, editors, Advances in Cryptology-Crypto'90, Vol. 537 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, pp. 627-638, 1990

[2] Eli Biham and Adi Shamir, "Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology4(1). pp. 3-72, 1991

[3] Kaisa Nyberg and Lars R. Knudsen, "Provable security against a differential attack", Journal of Cryptology8(1), pp. 27-37, 1995

[4] Mitsuru Matsui, "Linear cryptanalysis method for DES cipher", In Tor Helleseth, editor, Advances in Cryptology-Eurocrypt'93, Vol. 765 of Leture Notes in Computer Science, Springer-Verlag, Berlin, pp. 386-397, 1994

[5] R. D. Silverman, "A cost-based Security analysis of symmetric asymmetric Key lengths", Bulletin 13, RSA Lab., 2000

[6] D. E. Denning, "The data encryption standard : Fifteen years of public security", Dist. Lecture, 6th Annual Comp. Security Appl. Conf., IEEE Comp, Soc. Press, pp x - xv , 1990

[7] A. Shimizu, S. Miyaguchi, "Fast Data Encipherment Algorithm, FEAL", Proc. of Eurocrypt 91, 1991

[8] X. Lai, "On the Design and Security of Block Ciphers", ETH Series in Information Processing, Vol. 1, 1992

[9] E. Biham, A. Shamir, "Differential Cryptanalysis of Data Encryption Standard", Springer-Verlag, 1993

[10] C. H. Paradimitriou, Computational Complexity, Addison-Wesley, Reading, Massachusetts, 1994

[11] Bruce Schneider, "Applied Cryptography, Second Edition-Protocols, Algorithms, and Source Code in C", John Wiley & Sons, 1996

Seon-Keun Lee regular member

Journal of Electrical Engineering and Information Science Vol. 4, No. 6, Dec. 1999

Hwan-Yong Kim regular member

Journal of the korean institute of communication sciences, Vol. 26, No. 11B