논문 2007-44TC-3-8

갈로이스 부분장 변환을 이용한 새로운 고속의 경제적 치엔탐색기의 설계법에 대하여

(New Fast and Cost effective Chien Search Machine Design Using Galois Subfield Transformation)

안 형 근*, 홍 영 진**, 김 진 영***

(Hyeong-Keon An, Young-Jin Hong, and Jin-Young Kim)

요 약

리드솔로몬 복호기에서 4중 오류 이상의 오류치와 위치를 발견해 정정시는 보통 치엔탐색기를 사용한다. 이때 기존의 방법은 회로량이 많고 지연시간이 길어 비효율적이었다. 본 논문에서는 갈로이스 부분장을 이용 이 탐색기를 속도도 빠르고 회로량도 대폭 줄인 새로운 효율적 탐색기회로 설계법을 제시한다. 본 논문에서는 4중 오류위치를 정확히 추출함을 보였으나, 이 새 설계된 탐색기회로는 5중이상의 오류위치도 정확히 찾을 수 있는 설계이다. 새로운 회로는 정확히 오류위치를 발견할 수 있음이 예를 통해 검증되었다.

Abstract

In Reed Solomon decoder, when there are more than 4 error symbols, we usually use Chien search machine to find those error positions. In this case, classical method requires complex and relatively slow digital circuitry to implement it. In this paper we propose New fast and cost effective Chien search machine design method using Galois Subfield transformation. Example is given to show the method is working well. This new design can be applied to the case where there are more than 5 symbol errors in the Reed-Solomon code word.

Keywords: RS(Reed Solomon), Decoder, Error Locator polynomial, Galois Field(GF), Chien search machine, Newtonian Identities, Subfield Transformation, Number of Errors

I. Introduction

Reed Solomon coding theory is very famous well known nonbinary error correction method for Digital Electronic Devices (Consumer and Communication products.)[3].

In this paper, new RS(Reed Solomon) Decoder, which is correcting more than 4 symbol 1 errors, design method is proposed using Galois Subfield Transformation[5]. This method can be used when there are less than 4 error symbols, but in this case there are more efficient method which is described author's another paper[1,7].

In chapter 1 Introduction is written to introduce the whole paper. In chapter II, we briefly described how the Newtonian identities are used to determine the number of error symbols in the codeword. In

* 정회원, 동명대학교 정보통신과
(Dept. of Information and Telecommunication Engineering, Tong Myoung University.)

** 정회원, 동명대학교 전기및전자공학과
(Dept. of Electrical and Electronic Engineering, Tong Myoung University.)

*** 정회원, 동명대학교 메카트로닉스공학과
(Dept. of mechatronics Engineering, Tong Myoung University.)

접수일자: 2007년1월16일, 수정완료일: 2007년3월14일

chapter III we describe two types of classical Chien Search Machine design methods are described and two methods are compared from each other[9]. In Chapter IV we describes new efficient (fast and economical) chien search machine design method. The new design uses Galois subfield transformation from GF(2^4) to GF(2^8) field to simplify the Galois elements arithmetic operation[2].

Here we design various subcircuits, for example, **2 (Square), and **3(exponent power of 3) calculator circuits. The total number of gates and propagation delay is greately reduced compared with those of classical chien searchmachine described in chapter 3. In this chapter we proves that the new circuit is working well by finding 4 error locations of arbitralily given error locator polynomials which has 4 solutions corresponding to 4 error locations, using the new machine.

In chapter V future works that will be taken by us, and Comparisons between Old design and New design are described.

II. Error Locator polynomial and determination of number of error symbols in the RS codeword

The RS(Reed Solomon) codes are based on finite fields, often called Galois fields.

In CDP, RSC(32,28), on GF(2^8) field, code is used and up to 2 symbol errors can be corrected[1].

An RS code with 8bit symbols will use a Galois field GF(2^8), consisting of 256 symbols. In decoding Reed-Solomon code, we should calculate the Syndromes as in equation 1.

Let

$$C(X) = \Sigma_{j=0^{n-1}} C_j X^j$$

Be the Transmitted polynomial, and let

$$r(X) = \Sigma_{j=0^{n-1}} r_j X^j$$

Be the received polynomial. Then error pattern of the channel is

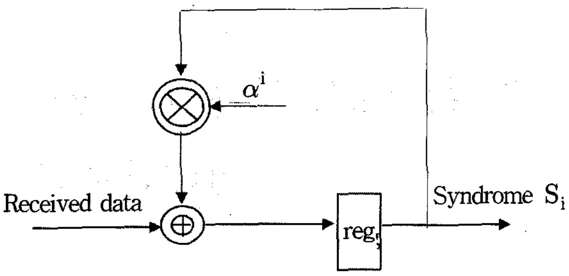


그림 1. RS 복부호기의 신드롬 계산기
Fig. 1. Syndrome calculator of RS codec.

$$E(X) = \Sigma_{j=0^{n-1}} E_j X^j$$

Where $E_j (j = 0 \text{ to } n-1)$ are error values. Here Syndromes are defined as

$$S_i = E(\alpha^i)(i = 0, 1, \cdots, 2t-1) \qquad (1)$$

For t error correction coding.

In this paper, for finding Error values and positions, syndrome calculator shown in Fig.1 is used[6].

Now if there are t errors, error values are E_n(n=0, 2···, t-1) and their positions are α^{jn}(n=0,1, ···, t-1).

Then Let

$$\beta_j (j = 0, 1, \cdots, t-1) = \alpha^{jn} (n = 0, 1, \cdots, t-1)$$

and Error Locator polynomial is defined as

$$\begin{aligned} \delta(X) &= (X - \beta_0)(X - \beta_1) \cdots (X - \beta_{t-1}) \\ &= \Sigma_{k=0}^{t} X^k \delta_{t-k} \end{aligned} \qquad (2)$$

Now Newton's identities are following set of equations.

$$\Sigma_{j=1}^{t} S_{t-j+v} \delta_j = S_{v+t} (v = 0, 1, 2 \cdots, t-1) \qquad (3)$$

These equations are for t error correcting Reed-Solomon codec[9]. Now let's define

$$A_i = [S_{v-I} S_{v+1-I} S_{v+2-I}]^T, \text{ for } i = 0,1,2,\cdots,v-1 \qquad (4)$$

Here If

$$F(v-1) = \det[A_0 A_1 A_2 \cdots A_{v-1}] \qquad (5)$$

Then if $F(v-1) \neq 00$ and $F(v) \equiv 0$, there are v errors in the One Reed Solomon codeword[4].

In these days, Equation (3) are solved using only 1 Multiplier and embedded Software coding to control the Main CPU core(Noramlly Arm core) of the system(Digital A/V system, for example, CDP, DAT, HDTV, etc.). So we get the coefficients δ_j 's of error locator polynomial (2).

III. Classical Chien Search Machine

In this section, we describe 2 types of currently used Chien search machine[4, 9]. The machine here and New design described in next section can be applied to finding any number of Errors in the code word.

1) First type

For less than 3 symbol errors in the RS ECC decoder, please see the Author's another paper[1, 3]. For more than 4 symbol errors in the RS codeword, we usually use Chien search machine shown in Fig. 2[9]. If Chien search machine is used for less than 3 symbol error case for RS decoder, it is very inefficient in speed and costwise. Chien search machine finds out all the solutions(i.e., error locations) of error locator polynomials, Equation (2) (in this case order of the equation is 4, so there are 4 solutions for the equation (6))[4]. Synchronized to the clock pulses, The Multipliers are connected to the D type F/Fs and They output α^{4i}, α^{3i}, α^{2i}, α^{i}[5]. So The machine's out Z becomes 0 when α^{I} is the solution (i.e. ,error location). In this way, the Machine finds out all 4 error locations sequentially (increasing order). Definitely for more than 5 error case, in same way the machine works.

Following Fig. 2. is a typical Chien Search Machine finding 4 symbol errors. But as you see, the circuitry is relatively complex and the speed is slow since everytime it iterates it requires accumulated multiplication, so becomes slow. The number of multiplier in GF(2^8) field is 7, and there are 4 8-bit Filpflops(Registers).

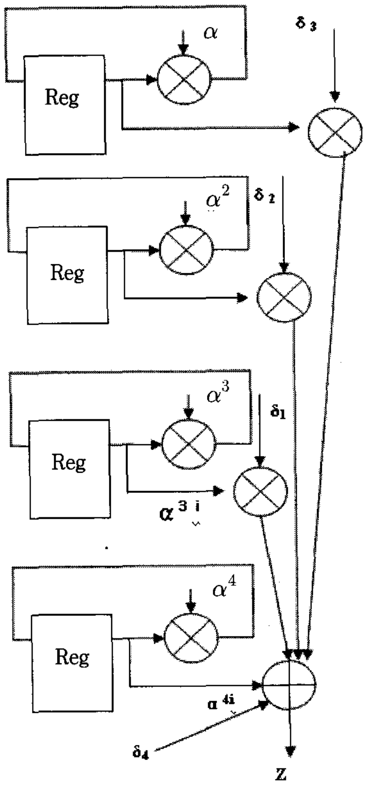


그림 2. 첫 번째 유형의 치엔 탐색기 구조圖 (4중 오류의 경우)

Fig. 2. Type 1 Classical Chien Search machine. (4 Error case)

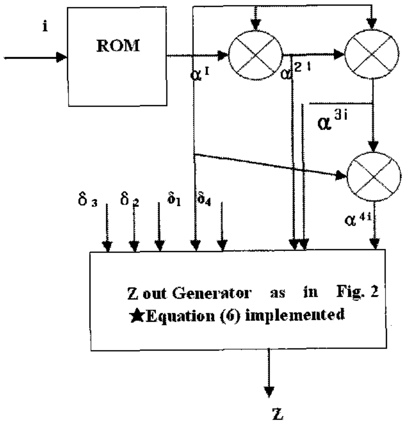


그림 3. 두 번째 유형의 치엔 탐색기 구조圖

Fig. 3. Type 2 Classical Chien Search machine.

The output $Z=\delta_4+\alpha^{I}\delta_3+\alpha^{2I}\delta_2+\alpha^{3I}\delta_1+\alpha^{4I}=0$, when α^{I} is correct error position.

The Gate Count for Z out Generator(Equation (6) is same as in Fig. 2. But I to α^{i} Transform ROM is anyway needed for other part of ECC block also, then Type 2 is definitely simpler than Type case (Type 2 needs only 3 Multipliers comparing 4 Multipliers of Type 1 case (excluding Zout cct) and no needs of Flip Flops. Also clock cycle period of type 1 is longer than 3 series propagation delays of type 2 case, so Type 2 Processing speed is faster than that of type 1.

$$Z = \delta_4 + \alpha^I \delta_3 + \alpha^{2i} \delta_2 + \alpha^{3I} \delta_1 + \alpha^{4I} \qquad (6)$$

Ⅳ. New Chien Search Machine Design for Reed-Solomon Decoder in GF(28)

In this chapter we describe new chien search machine structure using GF(2^8) to GF(2^4) Transformation[5]. Let's see Fig. 4 for the whole structure of the machine. The structure is composed of 3 parts (Transform part, HW of each exponent implementation, Z out generation part in GF(2^4)). Here we don't need Inverse transformation from GF(2^4) to GF(2^8), so resulting in additional saving the hw circuitry of the machine. The main idea of saving the HW circuit amount is the big simplification of HW circuit in GF(2^4) field and **2 circuit is much simpler than the multiplier circuit in GF(2^4) field[5].

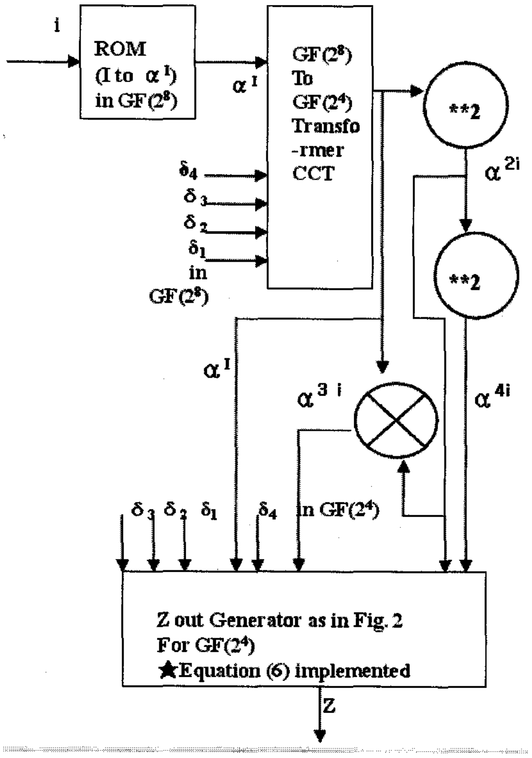


그림 4. 새로운 유형의 치엔 탐색기 구조圖 (4중 오류의 경우)

Fig. 4. New Chien Search machine Block Diagram. (4 symbol Error case)

Let's analyse the Circuit in Fig.4. There are 3 Kind of subcircuits in the machine. 1st Sub block is GF(2^8) to GF(2^4) Transfer circuit. The logic equation is as follows[5].

$$\text{IF } A = A0 + \beta A1, \text{ where } A,\ \beta \in GF(2^8)$$
$$\text{And } A0, A1 \in GF(2^4) \qquad (7)$$

Also $A = (b0, b1, b2, b3, b4, b5, b6, b7)$ and

$A0 = (Z0, Z1, Z2, Z3)$, $A1 = (Z4, Z5, Z6, Z7)$

$$\begin{aligned} Z0 &= b0 + b1 + b5 \\ Z1 &= b1 + b3 + b5 \\ Z2 &= b2 + b3 + b6 \\ Z3 &= b1 + b3 + b4 + b6 \\ Z4 &= b1 + b2 + b3 + b5 + b6 + b7 \\ Z5 &= b2 + b5 + b6 \\ Z6 &= b1 + b2 + b3 + b4 + b5 + b6 \\ Z7 &= b1 + b3 + b4 + b5 \end{aligned} \qquad (8)$$

Now Multiplier in GF(2^4) is IF

$$\begin{aligned} C &= AB \\ &= (A0 + \beta A1)(B0 + \beta B1) \\ &= (C0 + \beta C1) \end{aligned}$$

where A0,A1,B0,B1,C0,C1 $\in$ GF(2^4).

Then

$$\begin{aligned} C0 &= A0B0 + A1B1\ \lambda,\ \lambda \in GF(2^8) \\ C1 &= A0B1 + A1B0 + A1B1 \end{aligned} \qquad (9)$$

So the Multiplier in GF(2^4) requires 4 mutipliers over GF(2^4), 3 adders over GF(2^4) and a λ multiplier over GF(2^4). Now IF A=B, then equation (9) becomes **2 (Square) circuit in Fig. 4[5]. In this case(9) becomes equation (10) as follows.

$$\begin{aligned} C0 &= A0^2 + A1^2\ \lambda \\ C1 &= A1^2 \end{aligned} \qquad (10)$$

This circuit of equation (9) is really simple as if A0 =(x0,x1,x2,x3), $A0^2$ =(x0+x2+x3,x3,x1+x3,x2+x3) and λA0 is (x3,x0,x1,x2+x3), because λA0 is, when A0 = x0 + x1 λ + x2 λ^2 + x3 λ^3, x0λ+ x1 λ^2 + x2 λ^3 + x3 λ^4 =(x0+x2+x3,x3,x1+x3,x2+x3) and $A0^2$ is x0 + x1 λ^2 + x2 λ^4 + x3 λ^6 =(x0+x2+x3,x3,x1+x3,x2+x3) usingλ^4 = λ^3 + 1 (the primitive polynomial of GF(2^4). So $A0^2$ λ=(x2+x3,x0+x2+x3,x3,x1+x2)[5].

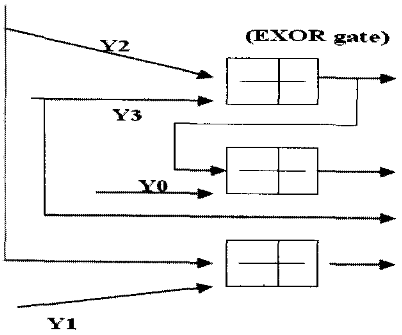


그림 5. A12 λ 형성회로
Fig. 5. A12 λ =(Y2+Y3,Y0+Y2+Y3,Y3,Y1+Y2) Circuit. **A1=(Y0,Y1,Y2,Y3).

So the equation (9) requires9 EXOR gates totally and A1^2 λ circuit is drawn in Fig.5.

<Example1>

If the Error locator polynomial over GF(2^8) is

$$\begin{aligned}&(x+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)\\&=X^4+X^3\delta_1+X^2\delta_2+X\delta_3+\delta_4\end{aligned}$$

So $\delta_1=\alpha^{76}, \delta_2=\alpha^{76}, \delta_3=\alpha^{81}, \delta_4=\alpha^{10}$.

These Values are normally calculated from Newtonian identity equations (3) using known Syndromes[8]. Now Find 4 correct error locations $\alpha, \alpha^2, \alpha^3, \alpha^4$ using New Chien Search Machine.

<Solution>

All $\delta_1(\mathrm{I}=1\ \mathrm{to}\ 4))$ and α^{I}(i=1)are transformed to GF(2^4) elements using equation (8) as follows[5].

$$\begin{aligned}&\delta_1=\alpha^{76}=\alpha^4+\beta\alpha^5\\&\delta_2=\alpha^{251}=\alpha^{10}+\beta\alpha^7\\&\delta_3=\alpha^{81}=1+\beta\alpha^{12}\\&\delta_4=\alpha^{10}=\alpha^{12}+\beta\alpha^{12}\ \ \text{Also}\\&\alpha^{\mathrm{i}=}\alpha=\alpha^5+\beta\alpha^{11}\end{aligned}$$

Now using Suare circuit (**2) and Multiplier circuit for Equations (9) and (10) in Fig.4, we find in GF(2^4) field

$$\begin{aligned}&\alpha^{2\mathrm{i}}=\alpha^2=\alpha^2+\beta\alpha^7\ \text{and}\\&\alpha^{3\mathrm{i}}=\alpha^3=\alpha^8+\beta\alpha^{11},\\&\alpha^{4\mathrm{i}}=\alpha^4=\alpha^3+\beta\alpha^{14}\end{aligned}$$

Finally Zout Generator detects whether out is zero or not as follows.

LSB Part in GF(2^4), $\alpha^{12}+\alpha^8+\alpha+\alpha^7+\alpha^3=0$ and MSB Part in GF(2^4), $\alpha^{12}+\alpha^7+\alpha^{11}+\alpha^9+\alpha^{14}=0$. So $\in$ GF(2^8) is really correct Error position. For α^{I}(i=2,3,4), we find They are also correct error positions.

★★ See EX2 for i=2 case !!

<Example 2>

For i=2 case : Now let's verify that α^2 is another Error location.

<Solution>

$\alpha^{\mathrm{i}}=\alpha^2=\alpha^2+\beta\alpha^7$ using Transform circuit, In Fig. 4 (Equation 8) and similarly,

$$\begin{aligned}&\alpha^{2\mathrm{i}}=\alpha^4=\alpha^3+\beta\alpha^{14}\\&\alpha^{3\mathrm{i}}=\alpha^6=\alpha^{14}+\beta\alpha^7\\&\alpha^{4\mathrm{i}}=\alpha^8=\alpha^{12}+\beta\alpha^{13}\end{aligned}$$

using Square circuit and Multiplier of Fig. 4 in GF(2^4). Now Finally we find Z out is also Zero and catch that α^2 is also Correct Error position.

V. Conclusion and Discussion

Classical Type 1 Chien machine is better for System synchronization control than Type 2 machine so more widely used than type 2 machine .

So here we compare type 1 and New Chien machine for gate counts and speed. Anyway Type2 is smaller than Type 1 machine, and has about 80% gate Counts. Type 1 machine and New machine has same Z generator equation. But gate countes are different from each other. If we assume F/Fs of Type 1 machine and ROM of new design have almost same size, so we 'd better compare the circuit section just after F/F and ROM(I to α^{i}) of two Chien machines. Table 1 shows the summary of 2 machine comparison.

Here We see our New Design is really Cost efficient (Gate Count of New design is about 57% gate count of the old design). Also, The speed of

표 1. 고전적 치엔 머신과새로운 치엔 머신의 회로소자(앤드와 엑스오아 게이트) 갯수 비교표

Table 1. Gate count Comparison between New design and Classical Chien machine.

	#of EXOR gates	# of ANDgates	Remark
Classical Type 1 machine	7X73 = 511	7X64=448	7 Multipliers in GF(2^8)
New Chien Machien	5X13+4X75+ 2X9=383	4X48=192	4 Multipliers and 2Squaring circuits (**2) in GF(2^4). Also GF(2^8) to GF(2^4) Transfer Circuit for δ_i s and α^i

New design is faster than that of Type 1 machine since propagation delay path is much shorter for New design than for Type 1.

Future Work is for Economic design of Reed Solomon Encoder[3]. Here we want to design very fast and low cost GF field Arithmatic operator circuit[2].

References

[1] 안형근, “디지탈 오디오/비디오, 통신용 전자기기를 위한 Reed - Solomon Codec 설계에 대해”, pp.13~18, 제42호, 2005년 11호 대한전자공학회지

[2] 심동욱, 권봉열, 안형근, “고속의 저비용 갈로이스 장원소간의 연산장치설계에 대해”, pp 112~117,제16권 제 1호, 2006년 2월 한국정보보호학회지

[3]. Hyeong-Keon An, TS Joo et al, “The New RS Ecc Codec For Digital Audio and Video”, IEEE CES Conference paper, PP112~115, 1992

[4] Lee Man Young, “BCH coding and Reed-Solomon Coding theory,” 1990, Minumsa (Daewoo Academic Press).

[5] US patent number 5227992, “Operational Method and Apparatus over GF(2m) using a Subfield GF(2m/2)”, Man-young Lee, Hyeong-Keon An et al., 1993 Jul. 13

[6] Kwang Y.Liu, “Architecture for VLSI design of Reed-Solomon Decoders,” IEEE Transactions on Computers. Vol.33, No.2, Feb. 1984.

[7] Hyeong-Keon An, “2 Error Correcting RS Decoder design”, IDEC Conference Paper, 2004.

[8] Hsu, I.K., I.S.Reed, “The VLSI Implementation of a Reed-Solomon Encoder Using Berlekamp’s Bit-Serial Multiplier Algorithm”, IEEE Trans. On Computer, Vol.C-33, No.10, pp.906-911(1984).

[9] Shu Lin, Daniel J. Costello, Jr., “Error Control Coding,” Prentice-Hall, pp.240~261(20044).

저 자 소 개

Hyeong-Keon An(정회원)

He received B. Engineering Degree in electrical engineering from Seoul National University, Seoul, KOREA, in 1979 and M. S degree in electrical science from Korea · Advanced Institute of Science and Technology, Seoul, Korea in 1981, and the Ph.D. degree in electrical engineering from State University of New York at Stony Brook, NY, USA., in 1988.

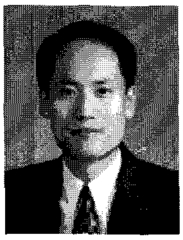
· In 1988, he joined Samsung Electronics Co.Ltd as a Senior Researcher working for designing · System LSI for 10 years.

· From 1998 to 1999 , He worked for Telson Electronics Corp. working for CDMA handphone design.

· In 2000, he joined Tong Myoung University in Busan as a Professor in Dept. Of Information and Telecommunication engineering.

· He has interests in designing CDMA and GSM hand phone and also in System LSI (Non Memory) design.

· He also operates Venture Company for Producing various Mobile devices and GPS/MP3 Engines, also OLED Displays.

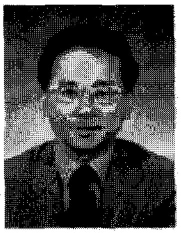


Jin-Young Kim(정회원)

· He received his B.S. degree from Seoul National University, Korea, his M.S. degree and his Ph.D. degree from Korea Advanced Institute of Science and Technology (KAIST), Korea.

From 1988 to 1998, he had worked for FA · Research Institute, Samsung Electronics Company Ltd., Korea. Since 1999, he has been a professor at the Department of Mechatronics Engineering, Tongmyong University, Korea.

His research interests include mechatronics, robotics and automation, intelligent control application.



Young-Jin Hong(정회원)

· He received the B. S. E. E. degree from Seoul National University. Seoul. Korea, in 1978 and the M. S. E. E. and Ph. D.(E. E.), from the State University of New York at Stony Brook in 1982 and 1985, respectively.

· From January 1986 until May 1986 he was with the Department of Electrical Engineering at the State University of New York ay Stony Brook, as an Assistant Professor. In June 1986 he joined LNR Communications, Inc., Hauppauge, NY, where he was a Research Staff Engineer and working on spread spectrum systems and satellite communications.

· In 1992 he came back to Korea to join Samsung Advanced Institute of Technology(SAIT), where he had been leading several research projects including CT2, VSAT and TDMA cellular basestations for two years.Since then he has broadened the spectrum of his career path to include not only the area of R&D(CTO of Eastel Systems from 1994 through 1997; CTO of Sungil Telecom in the year of 2004) sector but also the business rea(executive managing director of SKC&C from 1997 to 2003).

· He is currently an Associate Professor in the Department of Electrical and Electronics Engineering, Tongmyong University, Busan, Korea. His research interests are in the areas of smart antenna system, adaptive signal processing and communication systems.

· Dr. Hong is a member of Korean Institute of Communication Sciences, institute of Electronics Engineers of Korea. he is also a member of IEEE.