

차세대 DVB-RCS 시스템을 위한 저 계산량 연판정 e-BCH 복호 알고리즘

Low Computational Algorithm of Soft-Decision Extended BCH Decoding Algorithm for Next Generation DVB-RCS Systems

박태두 · 김민혁 · 임병수 · 정지원

Taedoo Park · Minhyuk Kim · Byeongsu Lim · Jiwon Jung

요 약

본 논문에서는 Chase 알고리즘 기반의 연판정 e-BCH 복호시 계산량을 감소하는 알고리즘을 제시하였다. Chase 알고리즘 기반의 연판정 e-BCH 복호 방식은 test pattern을 만들기 위해 수신 데이터 중 신뢰성이 낮은 데이터를 순서대로 찾기 위해 ordering을 한다. 데이터를 ordering하는 과정과 test pattern 수 만큼을 수신 데이터와 비교함으로써 최적의 복호 열을 찾는 과정에서 높은 복잡도가 요구되며, 본 논문에서는 이러한 복잡도를 줄이는 방안을 제시하여 계산량 및 성능 관점에서 비교 분석하였다.

Abstract

In this paper, we proposed the low computational complexity soft-decision e-BCH decoding algorithm based on the Chase algorithm. In order to make the test patterns, it is necessary to re-order the least reliable received symbols. In the process of ordering and finding optimal decoding symbols, high computational complexity is required. Therefore, this paper proposes the method of low computational complexity algorithm for soft-decision e-BCH decoding process.

Key words : Low Complexity Chase Algorithm, Soft-Decision e-BCH Code, Data Ordering

I. 서 론

초기의 DVB-RCS 표준안으로 채택되어진 이중이진 Turbo 부호의 성능이 오류 마루(error floor) 현상이 발생하여^[1], 이를 개선하기 위해 새로운 알고리즘들이 DVB-RCS NG(Next Generation)에서 제시되고 있다^{[2],[3]}. 새롭게 제시되고 있는 부호화 방식으로는 비선형 위성 채널에서 효율적인 CPM(Continuous Phase Modulation) 기반의 연판정 e-BCH(extended- BCH)

부호가 효과적임이 입증되었다. 기존의 경판정 e-BCH 복호 방식에서 Chase 알고리즘 기반의 연판정 e-BCH 복호 방식은 2 dB의 부호화 이득이 있으며^[4], 본 논문에서는 연판정 복호를 위한 chase 알고리즘^{[5],[6]} 기반에서 유래되는 복잡도를 줄이는 방안에 대해 연구를 하였다. 특히 연판정 e-BCH 복호시 필요한 Chase 알고리즘은 다음과 같은 단계를 나뉘어져 복호를 실행한다. 첫째 수신 데이터 중 신뢰성이 낮은 데이터를 찾아 test pattern을 생성하며, 생성된

「본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(계약번호 UD100002KD).」

「본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT 연구센터 지원사업의 연구 결과로 수행되었음(NIPA-2011-C1090-1121-0007).」

한국해양대학교 전파공학과(Department of Radio Communication Engineering, Korea Maritime University)

- 논문 번호 : 20110429-033
- 교신저자 : 정지원(e-mail : jwjung@hhu.ac.kr)
- 수정완료일자 : 2011년 7월 4일

test pattern을 수신 데이터와 ex-or-ing을 하기 위해 ordering시킨다. 둘째, ordering된 test pattern 수 만큼 e-BCH 복호를 행한다. 마지막으로 복호된 비트와 수신된 데이터를 이용하여 최적의 수신 비트를 찾아낸다. 최적의 수신 비트를 찾아내는 과정은 수신 데이터와 복호된 test pattern 수 만큼의 복호된 데이터와의 거리 차이를 이용하여 제일 작은 값을 복호된 비트라 간주하며, 스케일링 값과 신뢰도 값을 이용하여 반복하면서 복호한다. 본 논문에서는 다음과 같은 두 가지 단계에서 복잡도를 줄이는 방안을 제안한다. 첫째, test pattern을 구하기 위해 데이터를 ordering하는데 있어서 높은 복잡도가 요구되어지는데, 즉 부호화 비트의 길이를 N 이라 둘 때 $(N-1)!$ 의 연산량이 필요한데, 본 논문에서는 낮은 신뢰도의 한계치를 정하여 한계치 내에 신뢰성 없는 비트 p 개만 ordering함으로써 $(p-1)!$ 로 줄이는 방안을 제시하며, 둘째, test pattern 수 만큼을 수신 데이터와 비교하여 최적의 복호 비트열을 찾아내는 기존의 방식과는 달리, 신드롬 체크 후, 신드롬 값이 0이 되는 test pattern만 수신 데이터와 비교함으로써 계산량을 줄일 수 있다. 성능 분석 결과, 성능이 동일하면서 계산량이 감소됨을 알 수 있으며, 제시된 결과는 향후 DVB-RCS NG 시스템의 채널 부호화 방식에 대한 구현을 위한 설계 방안으로 유용한 자료가 되리라 사료된다.

II. DVB-NG에서 적용되는 e-BCH 부호화 방식

2-1 e-BCH 부호화 구조

Soft-decision BCH 부호는 그 구조가 매우 간단하고 복호과정이 RS 부호와 흡사하다. 또한 BCH 부호는 multiple random error correcting 능력을 갖추고 있다. 기본적으로 BCH 부호는 integers $m(m \geq 3)$ 과 에러 정정능력 $t(t < 2m - 1)$ 를 가지는데, 이 parameters를 이용하면 아래와 같은 식을 만들 수가 있다.

Block length : $n = 2^m - 1$
 Number of parity-check digits : $n - k \leq mt$
 Minimum distance : $d_{\min} \geq 2t + 1$ (1)

본 연구에서는 $n=63, k=51, t=2$ 인 (63, 51, 2) BCH 부호를 이용하여서 1 bit를 확장시킨 (64, 51, 2) e-

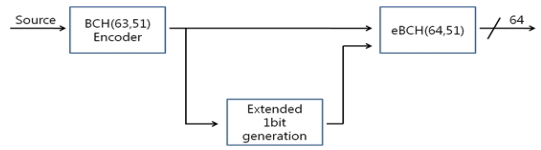


그림 1. e-BCH 부호화기
 Fig. 1. The encoder of e-BCH.

BCH 부호를 구성하였다. 1 bit를 확장시키는 방법에는 여러 가지 방법이 있지만, 본 연구에서는 (64, 51, 2) e-BCH 부호의 모든 bits를 ex-OR하는 방법을 고안하였다.

예를 들어 (63, 51, 2) BCH 부호의 부호어를 다음과 같이 표현하면,

$$C = [c_0 c_1 c_2 \dots c_{62}] \quad (2)$$

1 bit가 확장된 (64, 51, 2) e-BCH 부호의 부호어는 다음과 같이 표현될 수 있다.

$$C' = [c_0 c_1 c_2 \dots c_{63}] \quad (3)$$

여기서 확장된 c_{63} 부호는 모든 부호어의 ex-OR를 한 결과이므로 다음과 같이 표현된다. 부호화기의 구조를 보면 BCH(63, 51) 부호화기에서 인코딩을 한 후 마지막 비트를 식 (4)에 의하여 생성한다. 이는 수신된 심볼을 BCH 복호를 한 후 비록 신드롬이 0이 나오더라도 정확한 복호를 하였는지에 대한 check bit이다.

$$c_{63} = (c_1 + c_2 + c_3 + \dots + c_{62}) \text{ mod } 2 \quad (4)$$

또한 e-BCH 부호의 generation matrix는 아래와 같이 표현된다.

$$G_{k \times n}^{e-BCH} = [I_{k \times k} | P_{k \times (n-k)}] \quad (5)$$

2-2 연관정 e-BCH 복호화기 구조

그림 2는 연관정 e-BCH 부호화기와 복호화기의

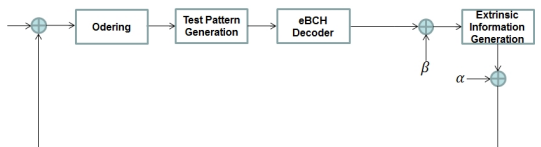


그림 2. Soft decision e-BCH 복호기 구조
 Fig. 2. The constructor of soft decision e-BCH.

구조를 나타낸다.

그림 2의 복호기의 구조를 전체적으로 설명하면, 수신된 심볼은 Chase II 알고리즘을 적용시키기 위해 test pattern을 생성한다. Test pattern은 p 개의 신뢰성 없는 수신 심볼에 “1”을 할당하고, 나머지는 모두 “0”으로 할당하여 $N_TP(=2^p)$ 개의 test pattern 심볼을 생성한다. N_TP 개의 test pattern 심볼과 수신 비트의 경관정 비트를 ex-OR하여 BCH 복호기에서 test pattern의 개수인 N_TP 만큼의 복호 심볼을 생성한다. N_TP 개의 복호된 비트열은 수신 심볼과 거리 차이를 구하여 N_TP 개 중 가장 거리가 짧은 부호열을 임의의 결정된 복호 비트(D)라 정의한다. 최적의 복호열 D 를 정하는 기존의 방식은 다음과 같이 요약 설명할 수 있다.

원 신호 E 그리고 가우시안 잡음 신호 N 에 의해 수신신호 벡터 R 에 대한 관계는 다음식과 같이 나타낼 수 있다.

$$R = E + N \quad (6)$$

여기에서

$$R = (r_1, r_2, r_3, \dots, r_n), \quad E = (e_1, e_2, e_3, \dots, e_n), \quad N = (n_1, n_2, n_3, \dots, n_n)$$

이다. 최적 결정 비트 $D = (d_1, d_2, d_3, \dots, d_n)$ 는 식 (7)과 같이 maximum likelihood 방식에 의해 결정된다.

$$D = C^i \text{ if } \Pr E = C^i | R > \Pr E = C^j | R \quad \forall j \neq i$$

$$D = C^i \text{ if } |R - C^i|^2 > |R - C^j|^2 \quad \forall j \neq i$$

$$|R - C^i|^2 = \sum_{i=1}^n (r_i - c_i^i)^2 \quad (7)$$

$C^i = (c_1^i, c_2^i, c_3^i, \dots, c_n^i)$ 는 가능한 모든 부호어의 집합 C 의 i 번째 부호어이다. 이 경우 n 값이 크면 계산량이 매우 많고 오래 걸리며 거의 불가능하다. 그러므로 해밍 거리의 범위에 존재하는 수신 비트열만 체크하는 Chase II 알고리즘을 이용하여 복호하여야 한다. 후보 가능한 부호어 C 를 찾는 Chase-II 알고리즘은 다음과 같다.

1단계 : $p = \left\lfloor \frac{\delta}{2} \right\rfloor$ 개의 신뢰성 없는 Y 의 비트 위치를 수신 벡터 R 을 이용해서 결정한다. 신뢰성 없는 비트의 위치는 다음과 같다.

$$\Lambda(y_i) = \ln \left[\frac{\Pr \left(e_j = +\frac{1}{r_j} \right)}{\Pr \left(e_j = -\frac{1}{r_j} \right)} \right] = \left(\frac{2}{\delta^2} \right) r_j = |r_j|$$

2단계 : q 개의 test pattern T^q 를 생성한다($q=2^p$). T^q 의 생성 방법은 n 개의 비트 위치 중 $\Lambda(y_i)$ 가 가장 적은 값에 해당하는 위치 j 에 “1”을 위치시키고, 나머지 비트 위치는 “0”을 삽입하며, $\Lambda(y_i)$ 가 가장 적은 두 개의 비트 위치에 “1”을 위치시키고, 나머지 비트는 “0”으로 배치한다. 같은 방법을 계속해서 $\Lambda(y_i)$ 가 가장 작은 개의 비트 위치에 “1”을 위치시키고, 나머지 비트는 “0”을 삽입한다. 그리고 항상 all-zero pattern을 항상 포함시켜야 한다.

3단계 : q 개의 T^q 를 생성하고 난 뒤에, $Z^q = Y \oplus T^q$ 하여 오류 위치를 정정한 Z^q 를 생성한다.

4단계 : Z^q 를 블록 복호하여 C^q 를 생성한다.

D 를 정의하면, 우선 반복 시 생성되는 r_j 의 soft decision 값 r'_j 는 입력 수신 벡터의 r_j 와 extrinsic 정보의 합으로서 표시될 수 있다.

$$r'_j = r_j + \alpha w_j \quad (8)$$

Extrinsic 정보 w_j 는 자기 신호 j 번째를 제외한 extrinsic 정보이며, 즉 r'_j 는 Chase 알고리즘에 의해 복호된 D 의 soft decision 값이며, β 는 신뢰도 factor이다.

$$r'_j = \beta d^j \quad (\beta \geq 0) \quad (9)$$

처음 반복 시에는 신뢰도가 낮으므로 낮은 값으로 반영하면서 반복 횟수가 증가할수록 높게 설정한다. α 는 스케일링(scaling) factor이며, 이는 수신 신호에 있는 샘플들의 표준편차를 고려한 것이다. 따라서 대부분의 논문에서도 $\alpha[m] = [0, 0.2, 0.2, 0.5, 0.7, 0.9, 1, 1]$, $\beta[m] = [0.2, 0.4, 0.6, 0.8, 1, 1, 1, 1]$ 으로 할당한다.

그림 3은 e-BCH 부호의 경관정 복호 및 연관정 복호 방식에 대한 성능 분석을 한 곡선이다. 연관정 복호 방식이 경관정 복호 방식에 비해 약 1.5 dB 정도의 부호화 이득을 얻을 수 있다. 그림 4는 연관정 BCH 복호시, test pattern 수에 따른 성능 분석이다. p 는 신뢰성이 없는 비트 수를 의미하며, $p=6$ 일 때에는 test

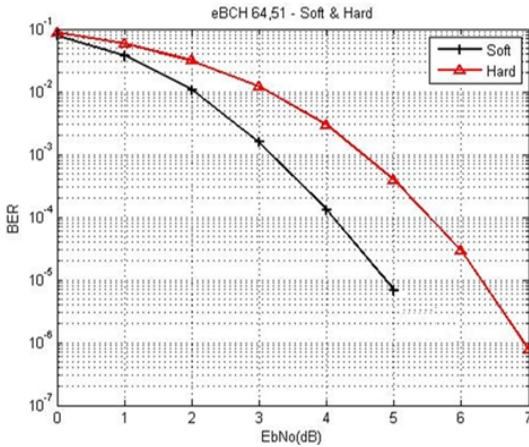


그림 3. e-BCH 64, 51 부호의 soft decision과 hard decision 성능 비교

Fig. 3. Performance comparison between soft decision and hard decision on e-BCH(64, 51) code.

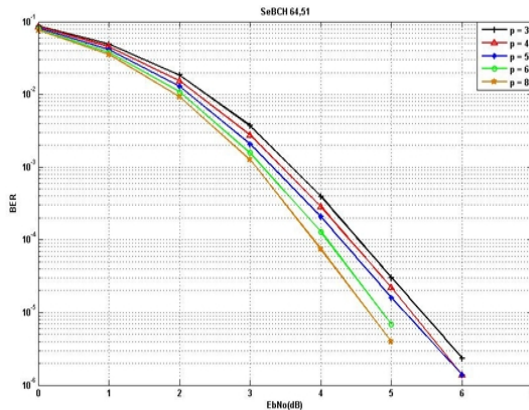


그림 4. e-BCH 부호의 p에 따른 성능 비교

Fig. 4. Performance comparison on 'p' of e-BCH code.

pattern 수는 2^p 개인 64개를 의미한다. p 가 증가할수록 성능이 향상됨을 알 수 있다.

III. e-BCH 부호의 복잡도 분석 및 개선 방안

그림 5는 제안한 e-BCH 수신부의 블록도를 나타낸다. 그림 2의 기존 복호기와의 차이점을 다음 두 가지로 요약이 된다.

첫째, test pattern은 p 개의 신뢰성 없는 수신 심볼을 생성하기 위한 ordering 과정에서 본 논문에서는 신뢰도 factor인 δ 를 설정하여, δ 보다 적은 값들에 대해서만 ordering을 한다. 시뮬레이션 결과 δ 를 0.4가

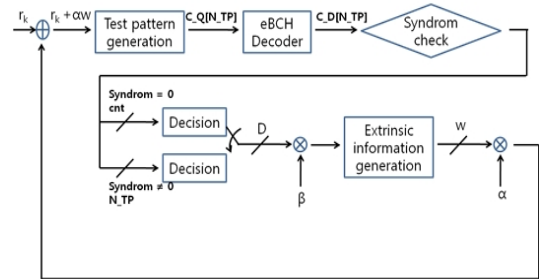


그림 5. 제안한 e-BCH 수신부의 블록도

Fig. 5. The block diagram of proposed e-BCH receiver.

최적임을 알 수 있었으며, δ 보다 작은 값들은 보통 p 개가 넘지 않는다는 것을 알 수 있었다.

제안한 ordering하는 과정은 다음과 같다.

```

C_Q[] = 0;
for(i=1; i<=N) if(R[]<delta) { pos[] = R[];
Ordering(pos[])
C_Q[pos[]] = 1;

```

Test pattern 출력 $C_Q[]$ 를 초기에 "0"으로 초기화시키고 N 개의 수신 심볼 중 δ 보다 작은 값들의 위치를 $pos[]$ 에 저장시켜, 저장된 $pos[]$ 를 낮은 값부터 ordering시킨다. 마지막으로 $pos[]$ 의 위치에 test pattern 심볼 $C_Q[] = "1"$ 을 할당한다. 따라서 기존 방식에서 모든 N 개의 심볼을 ordering하기보다는 한계치를 정하여 ordering함으로써 비교 함수가 $(N-1)!$ 에서 $(p-1)!$ 로 줄일 수 있다.

둘째로, 그림 5에서 N_{TP} 개의 test pattern 심볼 모두를 BCH 복호를 하지 않고 중간에 syndrome 검사를 하여 syndrome이 "0"이 되는 test pattern 수 만큼 최적의 복호 비트열 D 를 구하는 과정을 행한다. 만일 syndrome check를 하여 0이 존재하는 예비 복호 비트열이 존재하지 않을 때에는 기존의 방식과 같이 N_{TP} 개수만큼의 예비 복호 비트열 모두 최적의 복호 비트열 D 를 구하는 과정을 행한다.

IV. BER 성능 및 계산량 측면에서 분석

성능적인 측면에서는 기존의 방식과 계산량을 감소시킨 제안한 방식의 성능 차이는 거의 없음을 그림 6을 보면 알 수 있다.

계산량 측면의 관점에서 보면 1회 덧셈을 x 라 두

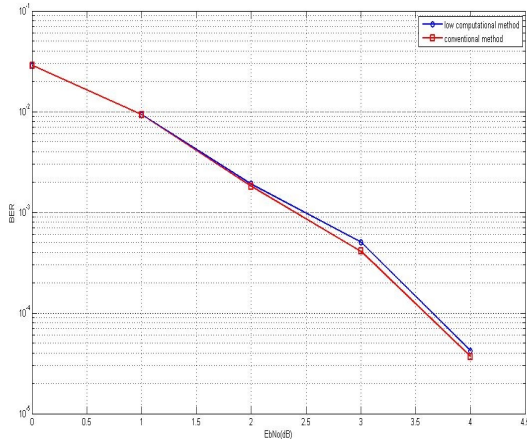


그림 6. Decision 블록에서 제곱 연산과 절대값 연산을 사용했을 때의 성능
 Fig. 6. The Performance of decision block using the square calculation and the absolute value.

면 기존의 계산량은 다음 식과 같다.

$$C=O((N-1)*x)+N_TP*B(x') \quad (10)$$

식 (10)에서 $O((N-1)*x)$ 는 ordering하는 과정에서 N 크기의 부호화된 수신 심볼을 처음부터 나머지 심볼을 비교하면서 제일 작은 값부터 ordering하는데, 각 심볼은 자신을 제외한 심볼들에 대해 비교를 행한다. 비교를 행하는 과정이 덧셈 1회라 설정할 수 있으므로, 총 $(N-1)!$ 만큼의 덧셈을 행한다. 또한 BCH 복호기에서 요구되는 덧셈 수를 x' 로 두었을 때, BCH 복호기의 계산량은 $B(x')$ 라 가정한다. N_TP 수($2p$) 만큼의 BCH 복호를 행함으로써, 식 (11)로 들 수 있다. 제안한 방식의 계산량은 아래 식과 같다.

$$C'=O(((p-1)!+N)*x)+N_TP*S(N*x)+q*B(x') \quad (11)$$

수신 심볼 N 개를 한계치와 비교함으로써 N 개의 덧셈이 필요하며, 이중 p 개를 ordering 함으로써, $(p-1)!$ 의 덧셈이 필요하여 총 $(p-1)!+N$ 개의 덧셈이 필요하며, syndrome 검사시, N 개의 덧셈이 필요하며, Galois Field 상에서의 곱셈은 LUT(Look Up Table)을 적용한다고 가정하였다. 따라서 syndrome 검사 시 필요한 계산량은 $N_TP*S(N*x)$ 이라 들 수 있다. N_TP 개의 test pattern을 syndrome 검사를 하므로 test pattern 중 syndrome이 0이 되는 q 개만 BCH 복호기에 입력되므로 $q*B(x')$ 라 들 수 있다.

결론적으로 식 (10)과 식 (11)을 비교하면 BER 성능이 그대로 유지하면서 계산량을 급격히 감소됨을 알 수 있다.

V. 결 론

본 논문에서는 연관정 복호를 위한 Chase 알고리즘 기반에서 유래되는 복잡도를 줄이는 방안에 대해 연구를 하였다. Test pattern을 구하기 위해 데이터를 ordering하는데 있어서 높은 복잡도가 요구되어지는데, 즉 부호화 비트의 길이를 N 이라 둘 때, $(N-1)!$ 의 연산량이 필요한데, 본 논문에서는 낮은 신뢰도의 한계치를 정하여, 한계치 내에 신뢰성 없는 비트 p 개만 ordering함으로써 $N+(p-1)!$ 로 줄이는 방안을 제시하였다. 시뮬레이션을 통해 기존 방식과 성능이 가장 근접한 한계치 값인 0.4로 할당하였다. 둘째, test pattern 수만큼을 수신 데이터와 비교하여 최적의 복호 비트열을 찾아내는 기존의 방식과는 달리, 신드롬 체크 후, 신드롬 값이 0이 되는 test pattern 만 수신 데이터와 비교함으로써 계산량을 줄일 수 있다. 여러 SNR값에 따라 syndrome이 0이 되는 test pattern 수가 틀리지만 보통 4~6개가 시뮬레이션을 통해 검증되었다. 성능 분석 결과, 성능이 동일하면서 계산량이 감소됨을 알 수 있으며, 제시된 결과는 향후 DVB-RCS NG 시스템의 채널 부호화 방식에 대한 구현을 위한 설계 방안으로 유용한 자료가 되리라 사료된다.

참 고 문 헌

- [1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes", *ICC93*, pp. 1064-1070, 1993.
- [2] C. Berrou, A. Graell, Amat, Y. Ould-Cheikh-Mouhamedou, C. Douillard, and Y. Saouter, "Adding a rate-1 third dimension to turbo codes", in *Proc. IEEE Inform. Theory Workshop*, pp. 156-161, Sep. 2007.
- [3] C. Douillard, C. Berrou, "Turbo code with rate- $m/(m+1)$ constituent convolutional codes", *IEEE Trans. Commun.*, vol. 53, no 10, pp. 1630-1638, Oct. 2005.

[4] Fijo Therattil Andrew Tangraj "A low-complexity soft-decision decoder for extended BCH and RS-like codes", *International Symposium on Information Theory*, pp. 1320-1324, 2005.

[5] R. M. Pyndiah, "Near-optimum decoding of product codes: Block turbo codes", *IEEE Trans. on Commu-*

nication, vol. 46, pp. 1003-1010, Aug. 1998.

[6] D. Chase, "A class of algorithms for decoding block codes with channel measurement information", *IEEE Trans.on Information Theory*, vol. IT-18, pp. 170-182, Jan. 1972.

박 태 두



2008년 2월: 한국해양대학교 전과 공학과 (공학사)
 2010년 2월: 한국해양대학교 전과 공학과 (공학석사)
 2010년 2월~현재: 한국해양대학교 전과공학과 박사과정
 [주 관심분야] 위성 통신, 이동 통신, 변·복조 기술, 채널 코딩, FPGA 기술 등

임 병 수



2011년 2월: 한국해양대학교 전과 공학과 (공학사)
 2011년 3월~현재: 한국해양대학교 전과공학과 석사과정
 [주 관심분야] 위성 통신, 이동 통신, 변·복조 기술, 채널 코딩, FP-GA 기술 등

김 민 혁



2006년 2월: 한국해양대학교 전과 공학과 (공학사)
 2008년 2월: 한국해양대학교 전과 공학과 (공학석사)
 2008년 3월~현재: 한국해양대학교 전과공학과 박사과정
 [주 관심분야] 위성 통신, 이동 통신, 변·복조 기술, 채널 코딩, FPGA 기술 등

정 지 원



1989년 2월: 성균관대학교 전자공학과 (공학사)
 1991년 2월: 성균관대학교 전자공학과 (공학석사)
 1995년 2월: 성균관대학교 정보공학과 (공학박사)
 1991년 1월~1992년 2월: LG 정보통신연구소 연구원
 1995년 9월~1996년 8월: 한국통신 위성통신연구실 선임연구원
 1997년 3월~1998년 12월: 한국전자통신연구원 초빙연구원
 1996년 9월~현재: 한국해양대학교 전과공학과 정교수
 2001년 8월~2002년 8월: 캐나다 NSERC Fellowship (Communication Research Center 근무)
 [주 관심분야] 위성통신, 이동통신, 변·복조 기술, 채널 코딩, FPGA 기술 등