

고정 부호율 극 부호의 성능 및 설계 방법

준회원 김 중 환*, 정회원 강 진 환*, 종신회원 김 상 호*

Performance and Construction of Polar Codes with Fixed Code Rate

Jong-hwan Kim* *Associated Member*, Jin Whan Kang* *Regular Member*,
Sang-Hyo Kim* *Lifelong Member*

요 약

2009년 Arikan에 의해 처음 제안된 극 부호(polar codes)는 실용적인 부·복호화 복잡도로 채널 용량을 달성하는 것이 증명된 채널 부호이다. 채널 양극화(channel polarization) 현상을 이용하는 극 부호는 현재 보안 및 데이터 압축 등에 응용되어 활발히 연구되고 있다. 본 논문에서는 극 부호의 실제 통신 시스템 적용을 고려하여, 유한한 길이와 고정 부호율을 갖는 극 부호의 설계 방법을 제안한다. 그리고 모의실험을 통하여 경험적으로 찾아낸, 가장 우수한 성능을 보이는 극 부호의 성능과 설계 방법을 제시한다.

Key Words : 극 부호(polar codes), 채널 양극화(channel polarization), 부호 설계(code construction), 연속 제거 복호(successive cancellation decoding)

ABSTRACT

In 2009, polar codes, proposed by Arikan, are theoretically proven codes to achieve capacity with acceptable encoding and decoding complexity. Currently, polar codes using channel polarization phenomenon are studied in security and data compression fields etc. In this paper, we consider the practical communication system and propose the construction method of polar codes with finite length and fixed code rate. Also, we show the outstanding performance and corresponding construction method of polar codes found by heuristic simulation.

I. 서 론

1948년 Shannon은 랜덤부호와 전형집합(typical set) 복호를 이용해 채널 용량을 달성하는 부호가 존재함을 증명하였다^[1]. 근래에 이르기까지 채널 용량을 달성하는 실용적인 부호를 찾지 못하고 있었는데, 1993년 이래 Turbo부호와 LDPC(low-density parity check)부호가 실용적인 부호 알고리즘으로 채널 용량에 근접한 성능을 갖도록 설계될 수 있음이 밝혀졌다.

2009년 Arikan은 채널 용량을 달성하며 실용적인

복잡도를 갖는 새로운 패러다임의 채널 부호, 극 부호(polar codes)를 제안하였다^[2]. 극 부호는 Turbo, LDPC 부호들과는 달리 광범위한 이진 입력 이산 무 기억 채널(discrete memoryless channel: DMC)에서 채널 용량을 달성함이 증명된 첫 번째 채널 부호라는 점에서 큰 의미를 갖는다. 뿐만 아니라 극 부호는 이론적 의미와 구조적 특성 상 다양한 문제에 접목될 수 있다는 장점을 가진다. 선행 연구에 의하면 극 부호는 Wiretap, 릴레이 채널에서도 채널 용량을 달성하며^[3,4], 연결 부호화 시스템의 외부 부호(outer code)로

※ 본 연구는 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행되었습니다.(2010-0010005).

* 성균관대학교 정보통신공학부 통신 및 부호이론 연구실(sas2323@skku.edu, jinhwan@skku.edu, iamshkim@skku.edu)
논문번호: KICS2011-03-133, 접수일자: 2011년 3월 3일, 최종논문접수일자: 2011년 6월 9일

도 연구된 바 있다⁵⁾. 뿐만 아니라 소스 부호화에도 적용되어 rate-distortion 한계 값을 달성하였다^{6,7)}.

본 논문에서는 정보이론 적으로 큰 의미가 있는 극 부호의 실제 점 대 점(point to point) 통신 시스템 적용을 고려한다. 유한한 길이와 고정 부호율을 갖는 극 부호의 설계 방법을 제안하며, 경험적으로 가장 우수한 성능을 보이는 부호 설계 방법을 제시한다. 모의실험에서는 이진 소실 채널(binary erasure channel: BEC)과 이진입력 부가백색 정규잡음 채널(binary-input AWGN channel: BIAWGNC)을 고려하며, 복호로는 [2]에서 제안된 연속 제거(successive cancellation: SC) 복호 기법이 사용된다.

II장에서는 극 부호가 이용하는 채널 양극화 현상에 대해 설명하며, III장에서는 기존의 극 부호 설계 방법과 고정 부호율을 기반으로 부호를 설계하는 방법을 설명한다. IV장에서는 모의실험 환경과 모의실험 결과를 설명하며, 마지막으로 V장에서는 본 논문을 요약하고 결론을 맺는다.

II. 채널 양극화

극 부호는 채널 양극화(channel polarization) 현상을 이용하여 채널 용량을 달성하는 부호이다. 채널 양극화는 N 개의 이진 입력 DMC에 대하여 채널 합성(channel combining)과 채널 분리(channel splitting)를 수행했을 때, 채널들의 대칭 용량(symmetric capacity)-이진 입력 0과 1을 동일한 확률로 전송했을 때 달성할 수 있는 채널 용량이 0 또는 1로 양극화되는 현상을 의미한다. 그림 1은 용량이 0.5인 BEC 1024개의 대칭 용량이 채널 합성과 분리를 통해 양극

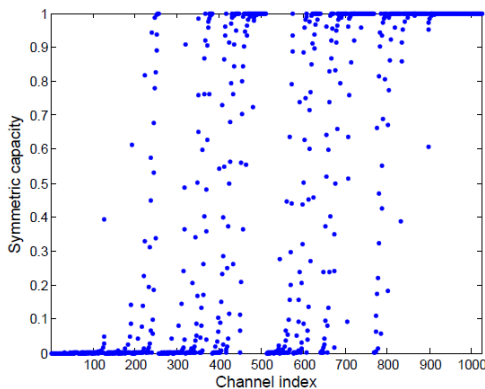


그림 1. 이진 소실 채널의 채널 양극화 현상 ($N=1024$)
Fig. 1. Channel polarization of binary erasure channel ($N=1024$)

화된 모습을 보여주고 있다. 본 장에서는 채널 합성과 채널 분리에 대해 소개하며, 채널 분리에 사용되는 SC 복호 기법을 설명한다. 채널 합성과 분리는 극 부호의 부호화와 복호화에 대응되며 이에 대한 그림은 그림 3에 나타나있다. 본 논문에서는 벡터 (u_1, \dots, u_j) 를 u_i^j 로 나타내며($j < i$ 일 경우, 벡터는 존재하지 않음), 이진 입력 대칭 DMC W 를 고려하도록 한다. 채널의 W 의 입력 x 와 출력 y 에 대해 천이 확률은 $W(y|x)$ 이며, N 개의 W 가 병렬로 있을 때 병렬 채널의 천이확률은

$$W^N(y_1^N|x_1^N) = \prod_{i=1}^N W(y_i|x_i) \text{으로 정의한다.}$$

2.1 채널 합성

채널 합성은 채널 W 를 재귀적으로 합성하여 길이 N 의 합성 채널을 만드는 과정이다. 두 개의 동일한 채널이 재귀적으로 합성되기 때문에 N 은 임의의 정수 n 에 대하여 $N=2^n$ 을 만족한다. 그림 2는 $N=4$ 일 때 채널 합성 과정을 보여주고 있다. 메시지 벡터 u_1^4 가 있을 때 u_i 성분끼리의 이진 덧셈(binary addition) 및 치환(permutation) 연산을 거쳐 x_1^4 가 생성되는 과정이 채널 합성이다. x_1^4 는 W^4 의 입력이 되며, y_1^4 는 W^4 의 출력이 된다.

채널 합성과정은 간단하게 행렬 G_N 을 통해 수행된다. 메시지 벡터 u_1^N 가 있을 때, W^N 채널의 입력은 $x_1^N = u_1^N G_N$ 가 된다. 여기서 G_N 은 x_1^N 를 생성하는 생성 행렬(generator matrix)이며, 식 (1)과 같이 정의 된다.

$$G_N = B_N F^{\otimes n} \tag{1}$$

B_N 은 [2]에서 정의된 bit-reversal 치환 행렬이며, $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $F^{\otimes n}$ 은 F 의 n 차 Kronecker power 연산을 의미한다. 합성된 채널은 W_N 으로 나타내며, 메시지

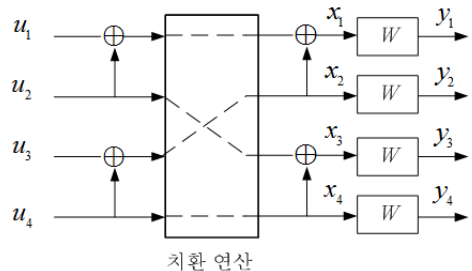


그림 2. 채널 합성 과정 ($N=4$)
Fig. 2. Channel combining phase ($N=4$)

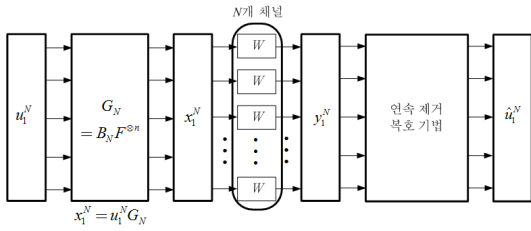


그림 3. 극 부호의 부호화 및 복호화 과정
Fig. 3. Encoding and decoding process of polar codes

벡터 u_1^N 와 채널의 출력 y_1^N 에 대한 W_N 의 전이 확률은 $W_N(y_1^N | u_1^N) = W^N(y_1^N | u_1^N G_N)$ 과 같다.

2.2 채널 분리

$u_1^N \in \{0, 1\}^N$ 이 균등한 분포(uniform distribution)를 갖는다고 하면, 합성 채널은 식 (2)와 같이 수학적으로 $\{W_N^{(i)} : 1 \leq i \leq N\}$ 으로 분리된다.

$$W_N^{(i)}(y_1^N, u_1^{i-1} | u_i) = \sum_{u_{i+1}^N} \frac{1}{2^{N-i}} W_N(y_1^N | u_1^N) \quad (1 \leq i \leq N) \quad (2)$$

Arikan은 N 이 커질수록 채널 $\{W_N^{(i)} : 1 \leq i \leq N\}$ 의 용량이 0 또는 1값에 가까워지고, 1에 가까운 채널의 비율이 채널 W 의 용량에 가까워짐을 증명하였다. 식 (2)는 수학적인 채널 분리를 보여주는데, 실제 이 과정은 고정비트의 전송과 SC 복호를 통해 유사하게 실현된다.

III. 극 부호 설계 방법

앞선 2장의 내용을 통해 채널 양극화는 채널 합성과 분리를 통해 수행되며, 채널 분리는 수신단이 알고 있는 고정 비트 값의 전송과 SC복호기로 유사하게 실현될 수 있음을 알아보았다. 극 부호를 설계한다는 것은 (2)에서 수학적으로 분리된 N 개의 채널 중 데이터를 전송할 K 개의 채널과 고정 비트를 보낼 $N-K$ 개 채널을 선택하는 작업이다. 이 때 데이터 채널로 채널 용량이 큰 K 개 채널들이 선택되며, K 개의 채널 인덱스 집합을 정보 집합(information set)이라고 한다. 이 때 부호율은 $R = K/N$ 이 된다. 본 장에서는 기존의 극 부호 설계 방법과 제안하는 부호 설계 방법에 대해 소개한다.

3.1 기존의 부호 설계 방법

Mori와 Tanaka는 대칭 채널 W 에 대하여 채널 합성-분리 과정을 이분(bipartite) 그래프로 표현하였다

[8]. 그리고 밀도 진화(density evolution)를 이용하여 새로운 채널 용량 비교 기준인 $P(A_{i,W})$ 을 제시하였다. $P(A_{i,W})$ 는 채널 W 에 대해서 $\hat{U}_i(y_1^N, u_1^{i-1}) \neq u_i$ 를 만족하는 모든 채널 입-출력의 경우에 대한 확률로, 각 채널 $W_N^{(i)}$ 의 비트 오류율을 나타낸다. 정보 집합을 I 로 표기한다고 했을 때, 특정 채널 W 에 대한 정보 집합 I_W 는 $I \subseteq \{1, 2, \dots, N\}$ 과 $|I| = K$ 을 만족하는 모든 I 에 대하여 $\sum_{i \in I} P(A_{i,W})$ 을 최소화하는 I 로 결정된다.

3.2 고정 부호율을 갖는 부호 설계 방법

극 부호를 실제 통신 시스템에 적용한다고 했을 때, 기존의 부호 설계 방법은 시스템에 바로 적용되기에는 부적합한 면이 있다. 왜냐하면 $\{P(A_{i,W}) : 1 \leq i \leq N\}$ 은 W 에 따라 변하는 값이기 때문에, 송신단이 정보 집합을 결정하기 위해서는 W 를 정확하게 알고 있어야 하기 때문이다.

본 절에서는 극 부호의 실제 시스템 적용에 초점을 맞춰 부호율이 고정된 극 부호를 고려하고, W 가 아닌 부호율 기반으로 극 부호를 설계하는 방법을 소개한다. Arikan은 N 이 무한으로 갈 때, 부호율이 R 인 극 부호가 $C(W) = R$ 을 만족하는 W 에 대하여 I_W 를 정보 집합으로 사용하면 채널 용량을 달성함을 증명하였다. 여기서 $C(W)$ 는 W 의 용량을 의미한다. 그러나 실제 시스템에서는 N 이 유한하기 때문에 I_W 를 정보 집합으로 사용하여도 채널 용량을 달성하지 못하고, 블록 오류가 발생하게 된다.

따라서 본 논문에서는 N 이 유한하고 부호율 R 이 고정됐을 때, 극 부호의 오류 성능 알아보기 위해 다음과 같은 두 가지 부호 설계 방법을 고려해본다. 첫 번째 방법은 부호율이 R 이고 N 이 유한할 때 $C(W) = R$ 을 만족하는 W 에 대하여 I_W 를 정보 집합으로 갖도록 극 부호를 설계하는 것이다. 그리고 두 번째 방법은 동일한 R 과 N 에 대하여 $C(\bar{W}) = \bar{R} > R$ 를 만족하는 \bar{W} 에 대하여 $I_{\bar{W}}$ 를 정보 집합으로 갖도록 극 부호를 설계하는 방법이다. 모의실험을 통해 두 가지 방법으로 설계된 극 부호의 성능 비교해 본다.

IV. 모의실험

본 논문의 모의실험에서는 3.2절에서 소개한 두 가지 방법으로 설계된 극 부호의 오류 성능을 비교해보고자 한다. $N=1024$ 와 2048 에 대해서 각각 부호율 R 이 0.5와 0.8로 고정된 부호를 고려한다. 그리고 모의

실험을 위해 BEC와 BIAWGNC를 사용한다. R 이 0.5인 부호 설계를 위해 BEC에서는 \underline{W} 와 \overline{W} 로 각각 채널 용량이 0.5와 0.7인 BEC(0.5)와 BEC(0.3)을 고려한다. 여기서 BEC(α)는 소실 확률이 α 인 채널을 가리킨다. BIAWGNC에서는 \underline{W} 와 \overline{W} 로 각각 채널 용량이 0.5와 0.74인 BAWGN(0dB)와 BAWGN(2.4dB)를 고려한다. 여기서 BAWGN(α dB)는 $E_b/N_0 = \alpha$ dB인 채널을 가리킨다. 그리고 그림에서 1024와 2048은 부호의 길이를 나타낸다. 특별히 $N=1024$ 일 때, \overline{W} 로 BEC(0.31)과 BAWGN(2.4dB) 채널을 고려한 이유는 두 채널을 기준으로 설계된 부호가 경험적으로 가장 우수한 성능 보였기 때문이며, $N=2048$ 일 때도 동일한 방법으로 채널들을 선택하였다. 마찬가지로 R 이 0.8인 부호를 설계하기 위해서 BEC에서는 부호의 길이에 따라 \underline{W} 와 \overline{W} 로 그림 5에 제시된 채널들을 사용하였다. 그리고 R 이 0.8인 경우에 대해 BIAWGNC에서 사용한 채널들은 그림 7에 제시되었다. 송신기에서

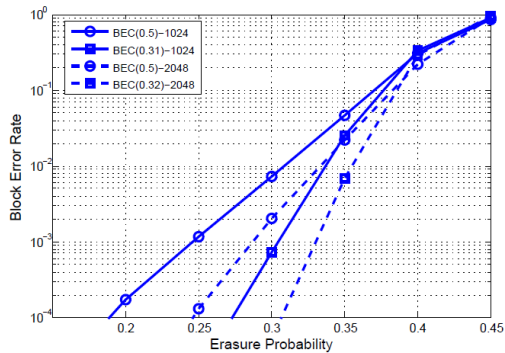


그림 4. BEC에서 각기 다른 채널로 생성된 부호율 0.5인 극 부호의 블록 오류율
Fig. 4. Block error rate of 0.5 rate polar codes constructed with different channels over BEC.

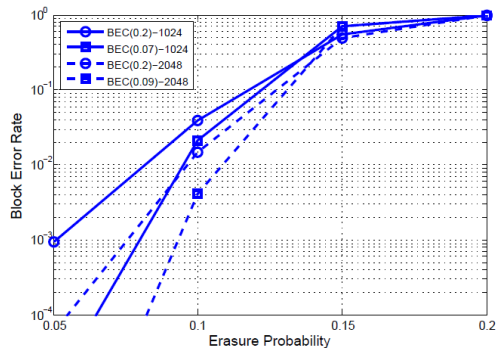


그림 5. BEC에서 각기 다른 채널로 생성된 부호율 0.8인 극 부호의 블록 오류율
Fig. 5. Block error rate of 0.8 rate polar codes constructed with different channels over BEC

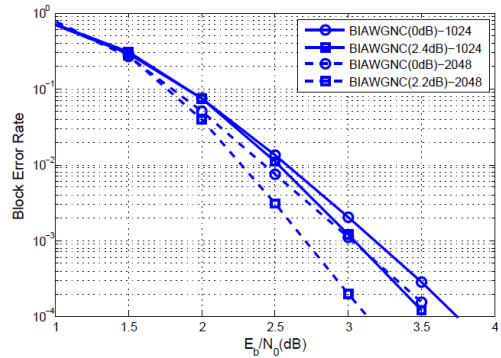


그림 6. BIAWGNC에서 각기 다른 채널로 생성된 부호율 0.5인 극 부호의 블록 오류율
Fig. 6. Block error rate of 0.5 rate polar codes constructed with different channels over BIAWGNC

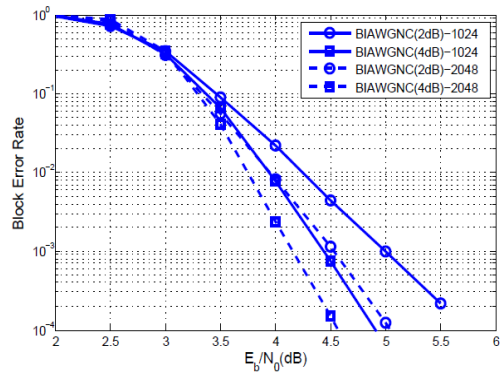


그림 7. BIAWGNC에서 각기 다른 채널로 생성된 부호율 0.8인 극 부호의 블록 오류율
Fig. 7. Block error rate of 0.8 rate polar codes constructed with different channels over BIAWGNC

부호 x_1^N 를 전송하면 수신기는 y_1^N 를 받아 \hat{u}_1^N 를 구하고 $\hat{u}_1^N \neq u_1^N$ 이면 블록 오류로 판단한다. 또한 블록 오류에 따른 재전송은 고려하지 않는다.

모의실험 결과가 그림 4~7에 나타나있다. 그림 4,5는 BEC에서 소실 확률에 따른 블록 오류율을 보여주고 있으며, 그림 6,7은 BIAWGNC에서 E_b/N_0 (dB)에 따른 블록 오류율을 보여주고 있다. 먼저 그림 4,5를 보면 BEC에서 채널 용량을 달성하는 $I_{\underline{W}}$ 로 설계된 부호보다 $I_{\overline{W}}$ 로 설계된 부호의 성능이 더 우수함을 알 수 있다. 마찬가지로 그림 6,7에서도 BIAWGNC에서 $C(\underline{W})=R$ 을 만족하는 채널 \underline{W} 를 기준으로 설계된 부호보다 $C(\overline{W})=\overline{R} > R$ 을 만족하는 채널 \overline{W} 를 이용해 부호를 설계하면 성능이 더 우수해질 수 있음을 확인할 수 있다. 이상의 결과를 통해 N 이 유한하고 고정

부호율 R 을 갖는 부호의 경우, 채널 용량을 달성하게 하는 정보 집합 $I_{\bar{w}}$ 가 오율 성능 측면에서 최적의 정보 집합이 아님을 알 수 있다. 즉, $C(\bar{w}) = \bar{R} > R$ 을 만족하는 적절한 채널 \bar{w} 를 선택하여 부호를 생성하면 어떠한 부호화 및 복호화 복잡도의 증가 없이, 채널 \bar{w} 로 부호를 설계 했을 때보다 오율 성능을 향상시킬 수 있음을 확인할 수 있다.

V. 결 론

본 논문에서는 극 부호를 실제 점 대 점 통신 시스템에 적용하는 것을 고려하여, 유한한 길이와 고정 부호율을 갖는 극 부호의 설계 방법을 제시하였다. 그리고 제시한 방법대로 설계된 부호들의 오율 성능을 비교하였다.

모의실험 결과에 따르면, 유한한 부호 길이 N 과 고정 부호율 R 을 갖는 부호가 있을 때, 채널 용량 달성을 위한 정보 집합을 선택하는 것이 오율 성능 관점에서 최선의 선택이 아님을 알 수 있었다. 채널 용량 달성을 기준으로 설계했을 때보다 $C(\bar{w}) = \bar{R} > R$ 을 만족하는 적절한 \bar{w} 를 기준으로 부호를 설계했을 때 더 우수한 오율 성능을 보임을 확인할 수 있었다.

차후에는 고정 부호율을 갖는 극 부호의 경우, 우수한 성능을 보장하는 정보 집합을 체계적으로 찾는 방법에 대한 연구가 필요할 것이다. 또한 다중 사용자 채널이나 페이딩 채널 등과 같은 실제 통신 시스템과 유사한 상황에서 극 부호의 성능을 확인하는 것이 필요할 것이다.

참 고 문 헌

[1] C. E. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, Vol.27, pp. 379 - 423, 623 - 656, July-Oct. 1948.

[2] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inform. Theory*, Vol.55, No.7, pp. 3051-3073, July 2009.

[3] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," arXiv:1001.0210v1, Jan. 2010.

[4] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, M. Skoglund, "Nested polar codes for

wiretap and relay channels," arXiv:1006.3573v1, Jun 2010.

[5] M. Bakshi, S. Jaggi, and M. Effros, "Concatenated polar codes," *IEEE Int. Symp. Inform. Theory*, June 2010.

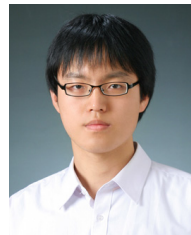
[6] N. Hussami, R.L. Urbanke, and S. B. Korada, "Performance of polar codes for channel and source coding," in *Proc. IEEE Int. Symp. Inform. Theory*, Seoul, South Korea, June 2009, pp.1488-1492.

[7] S. B. Korada and R. Urbanke, "Polar codes are optimal for lossy source coding," *IEEE Trans. Inform. Theory*, Vol.56, No.4, pp.1751-1768, April 2010.

[8] R. Mori and T. Tanaka, "Performance and construction of polar codes on symmetric binary-input memoryless channels," in *Proc. IEEE Int. Symp. Inform. Theory*, Seoul, South Korea, June 2009, pp.1496-1500.

김 종 환 (Jong-hwan Kim)

준회원



2010년 2월 성균관대학교 전자전기컴퓨터공학과 학사
 2010년 3월~현재 성균관대학교 전자전기컴퓨터공학과 석사과정
 <관심분야> 오류정정부호, 정보이론, 부호이론

강 진 환 (Jin Whan Kang)

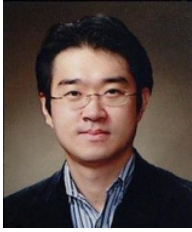
정회원



2008년 2월 성균관대학교 전자전기공학과 학사
 2010년 2월 성균관대학교 현대폰학과 석사
 2010년 3월~현재 성균관대학교 현대폰학과 박사과정
 <관심분야> 다중 안테나 시스템, 오류정정부호, 부호이론

김 상 호 (Sang-Hyo Kim)

중신회원



1998년 2월 서울대학교 전기공학부 학사

2000년 2월 서울대학교 전기공학부 석사

2004년 2월 서울대학교 전자·컴퓨터공학부 박사

2004년 3월~2006년 7월 삼성전자, 책임연구원

2006년 8월~2007년 8월 박사후 연구원(USC)

2007년 9월~현재 성균관대학교 정보통신공학부 조교수

<관심분야> 오류정정부호, 다중 안테나 시스템, 시퀀스, 협력 통신