직교 시퀀스를 이용한 양자통신에서의 효율적인 신호 검출 기법

김윤현*, 김진영* 정회원

Efficient Signal Detection Technique Using Orthogonal Sequence for Quantum Communication

Yoon Hyun Kim*, Jin Young Kim** *Regular Members*

요 약

우리나라는 지난 20여 년 디지털 정보기술 강국을 지향해 왔지만 선진국에서 이미 투자를 시작한 양자 정보 과학 분야에 대한 연구 및 투자는 거의 이루어지지 않았으며, 양자 정보 통신 기술의 수준 또한 개발 선진국들에 비해 턱없이 부족한 상황이다. 최근, 양자 역학에 기반을 두고 있는 양자 정보 처리 및 통신에 대한 연구가 세계적으로 활발히 진행 중이다. 90년대부터 본격화된 양자정보이론의 연구는 양자 컴퓨팅, 양자 통신, 양자 정보이론 등의 분야에서 발전해오고 있으며, 90년대 말에 이르러 양자 암호 통신 및 양자 알고리즘 등의 분야에서 큰 연구 성과를 나타내기 시작하였다. 본 논문에서는, 양자 통신 시스템에서 효율적인 양자 신호 전송 및 검출을 위해 직교 시퀀스를 이용한 효율적인 양자 신호 검출 방안에 대해 논하고자 한다.

Key Words : Quantum communication, signal detection, orthogonal sequence, auto/cross correlation

ABSTRACT

For the last 20 years, our country has been pointing to a great power for digital information technology, but quantum information technology which is already researched in many forefront nations lags significantly behind other countries. Recently, quantum information management, quantum computing and quantum communication based on the quantum mechanics have been researching actively in many fields such as cryptology. On the basis of these background, in this paper, to efficient data transmission and detection for quantum data, we apply the orthogonal sequence to quantum communication system. The performance of proposed scheme is analyzed in terms of auto and cross correlation performance.

I. 서론

최근, 양자 역학에 기반을 두고 있는 양자 정보 처리 및 통신에 대한 연구가 세계적으로 활발히 진행 중이다. 90년대부터 본격화된 양자정보이론의 연구는 양자 컴퓨팅, 양자 통신, 양자 정보이론 등의 분야에서 발전해오고 있으며, 90년대 말에 이르러 양자 암호 통신 및 양자 알고리즘 등의 분야에서 큰 연구 성과를 나타내기 시작하였다 [1-2].

1994년 피터 쇼어가 제시한 양자정보이론에 근거한 소인수분해 알고리즘과 1997년 그로버의 데이터 검색 알고리즘은 양자컴퓨터의 개념이 제안된 이후 처음으로 실용적인 측면에서 양자의 특성을 이용한 알고리즘이 가져올 가능성을 제시하였다 [3]. 이 가능성은 단순히 양자컴퓨터의 실용적 측면을 보여주는 동시에 양자 정보 이론의 발전을 통해 현재 구축된 기존 전산 시스템으로 구현된 암호체제가 붕괴될 수도 있기 때문에 세계 선진국 정보부서는 국가차원에서 양자 이론에 대한 연구지원을 서두르게 되었다.

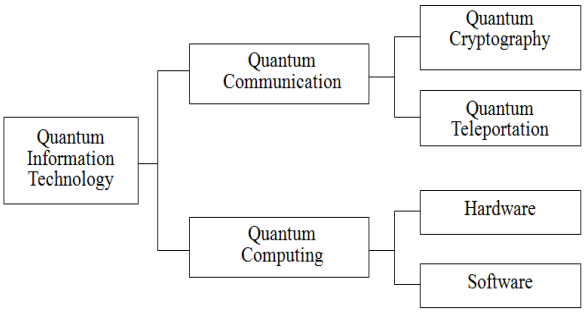


그림 1. 양자정보 통신 시스템의 적용 분야

광운대학교 전파공학과 소속 유비쿼터스 통신 연구실 (yoonhyun@kw.ac.kr), (jinyoung@kw.ac.kr)
접수일자: 2011년 2월 16일, 수정완료일자: 2011년 3월 19일, 최종게재확정일자: 2012년 6월 19일

최근 대규모 집적회로(VLSI) 기술의 비약적인 발전에 힘입어 보다 많은 정보를 더 신속하게 처리하게 할 수 있게 되었으며, 이를 위한 근간으로는 무엇보다 필수적으로 집적화 기술이 요구되었다. Moore 법칙에 의하면, 집적회로에 들어가는 트랜지스터의 수는 약 18개월마다 두 배로 증가한다고 하며, 이 법칙에 따르면 2020년경에는 칩의 고집적화로 인해 표면전기장(surface electronic field)의 증가로 potential well에 의한 양자현상을 피할 수 없는 상황에 도달하게 된다고 한다[4].

또한, Robert Kyeses가 연구한 정보 저장에 필요한 전자의 수를 시간의 흐름에 대해 분석한 자료에 따르면, 향후 20년 후면 1개의 원자에 1개의 비트를 저장할 수 있는 수준에까지 도달할 수 있을 것이라 한다 [5].

이렇게 머지않아 우리생활에 직접 이용될 양자현상을 이해하고, 양자계가 갖는 독특한 성질을 이용하고자 하는 연구가 증대되고 있다. 특히, 그림 1에서와 같이 현재보다 여러 가지 면에서 발전된 정보처리가 가능하다는 이론에 따라 정보처리 및 통신 분야에 양자역학을 적용해 보려는 연구가 많이 성행하고 있다.

이러한 흐름에 발 맞추어, 본 논문에서는 양자 통신 분야에서 송신 신호를 효율적으로 검출 할 수 있는 방안에 대해 분석하고자 한다. 본 논문에서 고려한 신호 검출 기법으로는 직교 시퀀스를 사용한 신호 검출 기법을 고려하였으며, 실험 결과로는 송신기에서 사용한 직교 시퀀스를 이용해 수신기에서 auto/cross correlation을 보여준다.

본 논문의 구성은 다음과 같다. 제 Ⅱ장에서는 양자 정보 통신 기술에 대한 간략적인 내용을 설명한다. 제 Ⅲ장에서는 본 논문에서 고려한 시스템 모델을 설명하고, 제 Ⅳ장은 직교 시퀀스를 적용한 모의실험 결과를 보여준다. 마지막으로 본 논문의 결론을 제 Ⅴ장에서 언급하였다.

Ⅱ. 양자 정보 통신 시스템

이번 장에서는 양자 정보 통시 시스템에서 사용되는 몇 가지 기본 개념들에 대해서 설명하도록 하겠다.

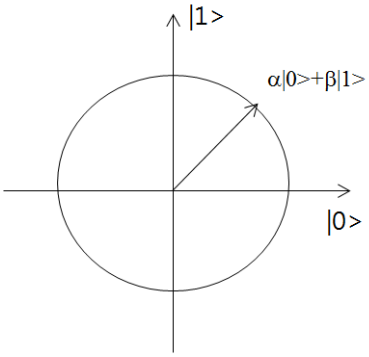


그림 2. Qbit의 벡터화

1. Quantum Bit

"Bit"는 기존 통신 시스템에서의 전송 및 정보 저장의 기본이 되는 단위이다. 하지만, 양자 정보 통신 시스템에서의 기본이 되는 단위는 더 이상 "bit"가 아니라 ""quantum bit (Qubit)" 이 라는 새로운 개념의 단위를 사용한다. 하나의 qubit은 '0'과 '1' 두 가지 상태를 표현 할 수 있으며, 각 각 |0>과 |1> 로 표현된다 [6-7]. 하지만, 기존의 bit 단위와는 다르게 qubit은, 그림 2에서와 같이 |0>과 |1> 두 상태를 동시에 표현 가능하며, 다음과 같이 나타낼 수 있다.

$$|\psi> = \alpha|0> + \beta|1> \quad (1)$$

여기서, α, β는 복소수 이다.

식 (1)에서와 같이, 하나의 qubit으로 두 개의 상태를 표현할 수 있는 중첩이 가능하며, 두 개의 상태 중에서 하나의 상태를 선택하는 것은 α, β에 의해 확률적으로 결정된다. 다시 말해, 상태 |0>으로 결정될 확률은 $\| \alpha^2 \|$ 이며, 반대로 |1> 로 결정될 확률은 $\| \beta^2 \|$ 이다. 또한, 확률의 기본 법칙을 만족하기 위해선 각 확률의 합은 1이 되어야 하며, 따라서 다음과 같은 수식을 얻을 수 있다.

$$\| \alpha^2 \| + \| \beta^2 \| = 1 \quad (2)$$

또한, 두 개 이상의 qubit 시스템에 대해서도 각각의 단일 qubit을 이용하여 표현 할 수 있다. "Bit" 단위에서의 두 개 bit의 표현 방법은 00, 01, 10, 11 이다. 이와 마찬가지로, "Qubit" 단위에서는 |00>, |01>, |10>, |11> 으로 표현되며 다음과 같이 나타낼 수 있다.

$$|\psi> = \alpha|00> + \beta|01> + \gamma|10> + \delta|11> \quad (3)$$

여기서, α, β, γ, δ는 복소수이며, 다음을 만족한다.

$$\| \alpha^2 \| + \| \beta^2 \| + \| \gamma^2 \| + \| \delta^2 \| = 1 \quad (4)$$

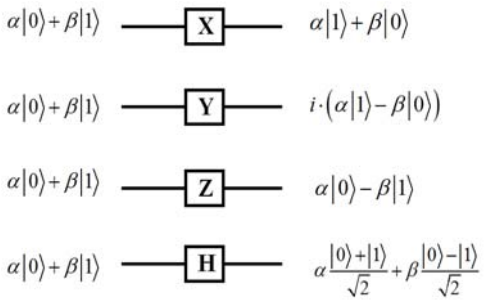
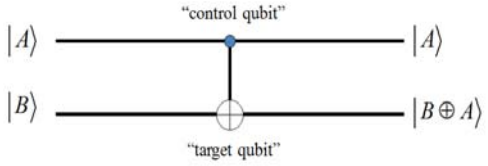


그림 3. 기본적인 quantum gate



$$\mathbf{CNOT}|00\rangle = |00\rangle$$
$$\mathbf{CNOT}|01\rangle = |01\rangle$$
$$\mathbf{CNOT}|10\rangle = |11\rangle$$
$$\mathbf{CNOT}|11\rangle = |10\rangle$$

그림 4. Quantum CNOT gate

2. Quantum Gate

이번 절에서는 기본적인 quantum gate에 대해 설명한다 [8-9]. 그림 3은 주요한 4개의 quantum gate를 보여준다. 기존의 NOT gate 와 유사하게, quantum X gate 는 단일 qubit의 상태를 천이시킨다. 따라서, 그림 3에서와 같이, $\alpha|0>+\beta|1>$이 quantum X gate를 통과하게 되면, $\alpha|1>+\beta|0>$의 출력값을 갖는다. 다음으로 quantum Z gate는 상태 |1>의 위상을 천이시킨다. 즉, quantum Z gate는 $\alpha|0>+\beta|1>$의 단일 qubit을 $\alpha|0>-\beta|1>$으로 천이시킨다. 그림 3의 quantum Y gate는 quantum X gate와 Z gate의 혼합형으로, 각 단일 qubit의 상태를 천이 시킴과 동시에, 상태 |1>의 위상을 천이시킨다. 마지막으로 quantum H gate는 가장 많이 쓰이고, 유용한 gate 중에 하나이다. Quantum H gate는 |0>을 $\frac{|0>+|1>}{\sqrt{2}}$로, |1>을 $\frac{|0>-|1>}{\sqrt{2}}$로 천이시킨다.

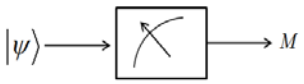


그림 5. Measurement gate

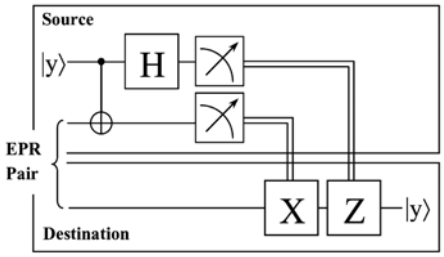


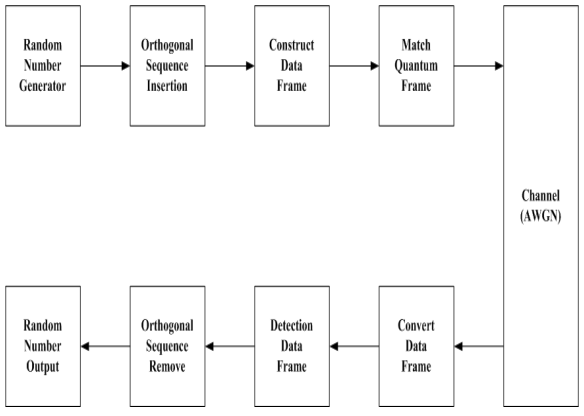
그림 6. Quantum Teleportation

그림 4는 quantum controlled-not (CNOT) gate를 보여준다. 그림 4에서 보이듯이, quantum CNOT gate는 두 개의 입력값을 가지며, 하나는 control qubit 이고 다른 하나는 target qubit 이라고 한다. Control qubit의 상태가 |0>이면, 입력값과 출력값은 동일하다. 하지만 control qubit의 상태가 |1>이면, 출력값의 target qubit는 입력값에 비해 다른 상태로 천이된다.

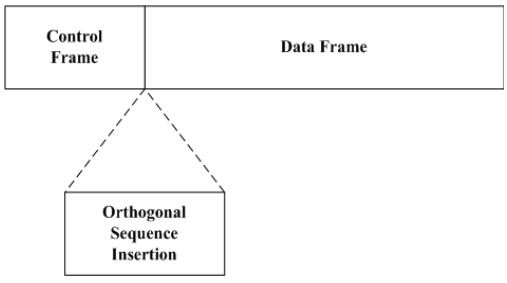
마지막으로, 그림 5는 입력 qubit에 대한 measurement gate를 나타낸다. Measurement gate는 임의의 qubit을 입력받아서 각 qubit의 상태 확률값에 따라 bit 형태로 판단해 주는 역할을 한다. 다시말해서, 만약 입력 qubit $|\psi> = \alpha|0>+\beta|1>$일 때, measurement gate에 의해서 $\| \alpha^2 \|$의 확률로 M은 0의 bit 값을 가지고, $\| \beta^2 \|$의 확률로 1의 bit 값을 갖는다.

3. Quantum Teleportation

Quantum Teleportation은 단일 또는 다수의 qubit의 상태를 특정 source에서 destination까지 전달하는 기술 중 하나이다 [10-11]. Quantum Teleportation은 source와 destination의 다리 역할을 해주는 EPR (Einstein, Podolsky, and Rosen) 쌍에 의해서 이루어진다. 그림 6은 quantum Teleportation의 구조를 나타낸다. 그림 6에서 단일 선은 qubit을 이중선은 bit의 이동경로를 의미한다. 그리고 각 source와 destination은 하나의 EPR 쌍을 공유한다. Source의 qubit |y>를 destination에 전달하기 위해서, 먼저 CNOT gate를 거친 후, H gate를 통과한다. 각 gate를 통과한 qubit은 measurement gate에 의해서 bit 단위로 변환되며, 각 bit를 이용하여 destination의 gate를 결정한다. 최종적으로 destination은 EPR 쌍을 이용하여 qubit |y>를 재 구성한다.



(a)



(b)

그림 7. 시스템 모델 (a) 전체 블록도 (b) 직교 시퀀스 삽입

Ⅲ. 시스템 모델

이번 장에서는 양자 통신 시스템의 시스템 모델과 본 논문에서 고려한 신호 검출 기법에 대해서 설명한다.

먼저 그림 7의 (a)는 본 논문에서 제안한 양자 통신 송신 송신부를 나타낸다. 먼저 각 송신부는 랜덤한 bit를 생성한 후 각 시스템이 원하는 전송 data를 형성한다. 이 때, 그림 7의 (b) 에서와 같이, 보내고자 하는 frame에 직교 시퀀스를 삽입한다. 즉, 보내고자 하는 frame의 data frame과 control frame 사이에 직교 시퀀스를 삽입한다. 이 때, 삽입되는 직교 시퀀스는 시스템의 성능, 즉 데이터 속도 및 기타 성능을 크게 저하 시키지 않는 범위에서 직교 시퀀스의 크기가 결정된다. 자세한 삽입되는 직교 시퀀스의 길이는 다음장에서 설명한다.

그 후 각 data는 전송하고자 하는 quantum channel에 알맞은 형태의 quantum data로 치환된다. 그림 7 (a)에서의 "Match Quantum Data" 블록에서는 앞서 Ⅱ 장에서 설명한 각 quantum gate 들이 단독 또는 조합되어 quantum data를 형성시키며, 본 논문에서는 간단한 quantum H gate를 이용하였다.

수신부에서는 우선 시스템의 성능을 높이기 위하여, 본 논문에서는 송 수신단 사이에 발생하는 간섭은 없다고 가정하였다. 그 후, quantum data를 복구하고 송신단에서 삽입된 직교 시퀀스를 이용하여 각 송신단의 신호를 검출한다.

본 논문에서는 일반적인 AWGN (additive white Gaussian noise) 채널 모델을 이용하였으며, AWGN 채널을 통과한 직교 시퀀스가 삽입된 수신 신호 $r(n)$은 다음과 같이 표현 할 수 있다.

$$r(n) = h^i(n) \otimes x(n) + n(n), \tag{1}$$

여기서 $h^i(n)$는 각 송신 데이터가 통과하는 채널을 나타내고, $x(n)$은 직교 시퀀스가 삽입된 송신 데이터를, 마지막으로 $n(n)$은 AWGN를 나타낸다.

수신단의 detection data frame 블록에서, 삽입된 원래의 직교 시퀀스를 이용한 자기 상관 함수를 이용한 log-likehood 함수를 이용하여 다음과 같은 식을 얻을 수 있다.

$$L(S) = \ln p(r(n)) \tag{2}$$

여기서 $p(r(n))$은 수신신호의 PDF(power spectrum density)를 나타낸다.

위의 식 (2)로부터, 삽입된 직교 시퀀스를 이용한 다음과 같은 ML (maximum likelihood)를 얻을 수 있다.

$$\hat{S} = \arg\left\{\max_S L(S)\right\},$$

$$= \arg\left\{\max_S \sum_{n=0}^{i-1} \ln\left(p\left(r(n)\right)\right)\right\}, \tag{3}$$

$$= \arg\left\{\max_S \sum_{n=0}^{2i-1} r(n) w(\tau - n)\right\}$$

여기서 $w(n)$은 송신부에서 삽입되었던 직교 시퀀스를 나타낸다.

최종적으로 삽입되었던 직교 시퀀스를 제거 한 후, 원래의 random bit로 변환 시킨다.

Ⅳ. 모의 실험 및 결과

표 1. 모의 실험 파라미터

Parameters	Value
Orthogonal sequence	Kasami sequence, M-sequence, PN sequence
Sequence length	500
Noise model	AWGN
Quantum gate	Quantum **H** gate

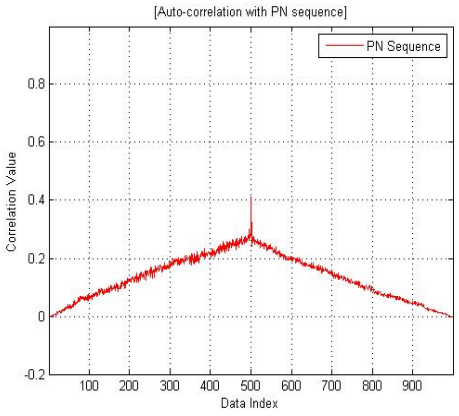


그림 8. PN sequence를 이용한 신호 검출 성능

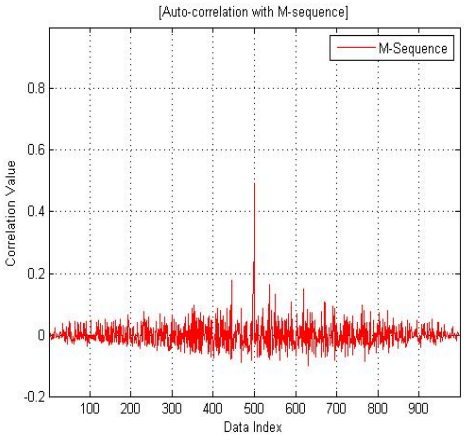


그림 9. M-sequence를 이용한 신호 검출 성능

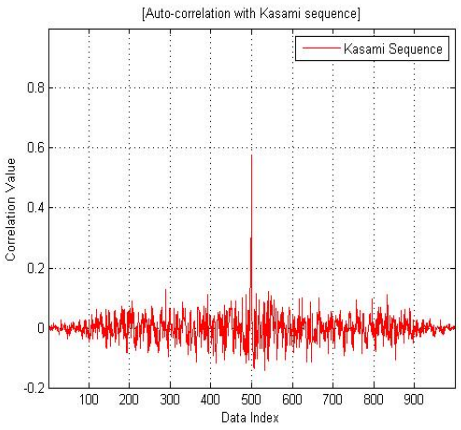


그림 10. Kasami sequence를 이용한 신호 검출 성능

본 논문에서 고려한 노이즈 모델은 백색 잡음 (AWGN, additive white Gaussian noise)으로 설정하였다. 또한 본 논문에서 사용한 직교 sequence로는 Kasami sequence, M-sequence, 그리고 PN sequence를 이용하였다. 각 sequence의 길이는 총 500 bit로, 각 100bit 씩 나누어서 5개의 data frame에 삽입하였다. 수신단에서는 5개의 프레임을 수신한 후 각 프레임의 직교시퀀스를 추출하여 자기 상관 함수를 이용해 송신 신호를 추출한다.

그림 8은 PN sequence를 이용한 수신단의 신호 검출 성능이다. 신호 검출 성능은 자기 상관 값으로 표현된다. 그림 8의 PN sequence의 경우, 자기 상관 peak와 주위의 side-lobe 값의 차이가 심하지 않다. 즉, 다시말해, main peak에 비해 side-lobe 값 또한 많이 커서, 효율적인 신호 검출이 이루어지지 않을 수 있다.

이러한 단점을 해결하기 위해 그림 9와 그림 10은 M-sequence와 Kasami sequence를 이용한 신호 검출 성능을 보여준다. 실험 환경은 그림 8과 동일하다. 그림 9와 10에서 보이듯이, main peak 값이 0.5를 상회하는 성능을 보일 뿐만 아니라, main peak와 side-lobe의 차이도 상당히 큰 것을 알 수 있다.

V. 결론

본 논문에서는 양자 통신 시스템의 기본적인 몇 가지 개념들과 다중 사용자 간 간섭이 존재할 경우 간섭에 대한 시스템의 악 영향을 줄일 수 있는 방안에 대해 연구하였다. 국내에서는 관련분야의 필요성 및 가능성이 강조되어 왔으나 대부분의 연구가 양자암호통신 분야에 국한되어 있으며 물리학에 근거한 양자 광학 및 반도체 물성 분야를 제외하고는 양자 정보 이론 및 양자 정보 통신의 기초 개념과 같은 양자 정보 이론의 기반조차 정립되어 있지 않은 실정이다. 이와 같이 양자 정보 이론을 비롯한 양자 관련 분야는 양자 통신을 통한 고전적인 채널 용량의 한계 극복 등의 연구가 향후 20년 이내에 구체화 될 것으로 예상된다. 실제로 이와 관련된 연구가 선진 각국에서 현재 활발히 진행되고 있으며, 아울러 학계 간 연계연구의 중요성을 인지함으로써 수학, 전산학, 물리학, 공학 등 여러 분야에서의 활발한 교류가 이루어지고 있다. 따라서 각국의 지원 규모와 특허 상황 등을 이용하여 현재 국내외에서 진행되고 있는 양자 정보 처리 및 통신 관련 연구 분야와 각국의 연구 동향을 분석하고, 이를 바탕으로 국내 양자 정보 처리 및 통신에 대한 연구 방향 수립이 필요하다.

참 고 문 헌

[1] Brooks, M. (Ed.) Quantum Computing and Communications, Springer, 1999.
[2] V.W.S. Chan, "Optical space communications," IEEE Journal on Selected Topics in Quantum Electronics, vol. 6, Dec. 2000, pp. 959-975.
[3] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring,"in Proc. 35th Annu. IEEE Symp. Foundations Comput. Sci.,1994, pp. 124 - 134.
[4] G.E. Moore, Electronics, Vol. 38, No. 7, 1965, p. 114 .
[5] R.W. Keyes. IBM. J. Res. Dev. 32, Vol. 24, 1988, p. 24.
[6] Tzong S., C.Y. Wang, and Ming-Hon Tao. "Quantum communication for wireless WAN," IEEE, Vol. 23, No. 7, 1425-1432 July 2005.
[7] Nayak A., J. Salzman, "On communication over an entanglement assisted quantum channel," in Proc.34th Annu. ACM Symp. Theory Comput., May 2002, pp. 689 - 704.
[8] C.H. Bennet, "Quantum information and compuation,"Phys. Today, Vol. 48, No. 10, Oct. 1995, pp. 24 - 30.
[9] S. Wieder, The Foundations of Quantum Theory, Academic Press, 1973.
[10] E. Hagley et al., "Generation of Einstein-Podolsky-Rosen Pairs of atoms,"Phys. Rev. Lett. 79, 1997. pp. 1 - 5.
[11] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge, Cambridge University Press, 2000.

저자

김 윤 현(Yoon Hyun Kim)

- 2006년 2월: 광운대학교 전파공학과 졸업
- 2008년 2월: 광운대학교 전파공학과 석사 졸업
- 2008년 3월~현재: 광운대학교 전파공학과 박사과정

<관심분야> : 디지털 통신, 협력통신, 가시광 통신, Cognitive Radio

김 진 영(Jin Young Kim) **정회원**

- 1998년 2월: 서울대학교 전자공학과 공학박사
- 2000년: 미국 Princeton University Associate
- 2001년: SK 텔레콤 네트웍 연구소 책임연구원
- 2009년~2010년 2월: 미국 M.I.T 공대 Visiting Scientist
- 2001년~현재 : 광운대학교 전파공학과 교수

<관심분야> : 디지털 통신, 유무선통신 시스템, 채널부호화, 인지무선 통신, 차세대 이동 통신 시스템